frontline
Debug Communications Faster™

ComProbe User Manual

Revision Date: 12/15/2015

Copyright © 2000-2015 Frontline Test Equipment, Inc.

FTS, Frontline, Frontline Test System, ComProbe Protocol Analysis System and ComProbe are registered trademarks of Frontline Test Equipment, Inc.

The following are trademarks of Frontline Test Equipment, Inc.

The Bluetooth SIG, Inc. owns the Bluetooth® word mark and logos, and any use of such marks by Frontline is under license. All other trademarks and registered trademarks are property of their respective owners.

Contents

Chapter 1 ComProbe Hardware & Software **1**
1.1 What is in this manual 2
1.2 Computer Minimum System Requirements 2
1.3 Software Installation 2
1.3.1 From CD: 2
1.3.2 From Download: 3
Chapter 2 Getting Started **4**
2.1 802.11 Hardware 4
2.1.1 Connecting/Powering the ComProbe 802.11 5
2.1.2 Setting Up for ProbeSync™ 6
2.2 Data Capture Methods 7
2.2.1 Opening ComProbe Data Capture Method 7
2.2.2 ComProbe 802.11 Air Sniffing Data Capture Methods 9
2.2.3 Bluetooth® /802.11 Air Sniffing Multiple Technologies Aggregated. 10
2.2.4 Virtual Sniffing 10
2.2.5 Determining Master and Slave 11
2.3 Control Window 11
2.3.1 Control Window Toolbar 12
2.3.2 Configuration Information on the Control Window 13
2.3.3 Status Information on the Control Window 13
2.3.4 Frame Information on the Control Window 13
2.3.5 Control Window Menus 14
2.3.6 Minimizing Windows 17
Chapter 3 Configuration Settings **18**
3.1 802.11 Configuration 18
3.1.1 ComProbe 802.11 Hardware Settings 18
3.1.2 802.11 I/O Settings 18
3.1.2.1 Settings 19
3.1.2.2 Status 21
3.1.2.3 Capture Filters 21

3.1.2.4 Firmware Update 23
3.1.2.5 Security 25
3.1.2.6 Wi-Fi Device Scanner 25
3.1.3 Wi-Fi Device - MAC Address Editor 29
3.2 Decoder Parameters 29
3.2.1 Decoder Parameter Templates 31
3.2.1.1 Select and Apply a Decoder Template 31
3.2.1.2 Adding a New or Saving an Existing Template 32
3.2.1.3 Deleting a Template 32
3.2.2 Wi-Fi Security Decoder Parameters 33
3.2.3 Adding or Changing TCP/UDP Port Assignments 35
Chapter 4 Capturing and Analyzing Data 37
4.1 Capture Data 37
4.1.1 Air Sniffing: Positioning Devices 37
4.1.2 Capturing Data to Disk - General Procedure 39
4.1.2.1 ComProbe 802.11 with Wireshark® 41
4.1.3 Capturing Using Frontline Wi-Fi Datasource with Wireshark® 41
4.1.4 Combining BPA 600, 802.11, and HSU with ProbeSync 44
4.1.5 Extended Inquiry Response 46
4.2 Protocol Stacks 46
4.2.1 Protocol Stack Wizard 47
4.2.2 Creating and Removing a Custom Stack 48
4.2.3 Reframing 49
4.2.4 Unframing 49
4.2.5 How the Analyzer Auto-traverses the Protocol Stack 50
4.2.6 Providing Context For Decoding When Frame Information Is Missing 50
4.3 Analyzing Byte Level Data 51
4.3.1 Event Display 51
4.3.2 The Event Display Toolbar 52
4.3.3 Opening Multiple Event Display Windows 54
4.3.4 Calculating CRCs or FCSs 54

4.3.5 Calculating Delta Times and Data Rates 55
4.3.6 Switching Between Live Update and Review Mode 55
4.3.7 Data Formats and Symbols 56
4.3.7.1 Switching Between Viewing All Events and Viewing Data Events 56
4.3.7.2 Switching Between Hex, Decimal, Octal or Binary 56
4.3.7.3 Switching Between ASCII, EBCDIC, and Baudot 57
4.3.7.4 Selecting Mixed Channel/Sides 57
4.3.7.5 List of all Event Symbols 58
4.3.7.6 Font Size 60
4.4 Analyzing Protocol Decodes 60
4.4.1 Frame Display Window 60
4.4.1.1 Frame Display Toolbar 63
4.4.1.2 Frame Display Status Bar 66
4.4.1.3 Hiding and Revealing Protocol Layers in the Frame Display 66
4.4.1.4 Physical vs. Logical Byte Display 67
4.4.1.5 Sorting Frames 67
4.4.1.6 Frame Display - Find 67
4.4.1.7 Synchronizing the Event and Frame Displays 69
4.4.1.8 Working with Multiple Frame Displays 70
4.4.1.9 Working with Panes on Frame Display 70
4.4.1.10 Frame Display - Byte Export 70
4.4.1.11 Panes in the Frame Display 72
4.4.1.11.1 Summary Pane 72
4.4.1.11.2 Customizing Fields in the Summary Pane 75
4.4.1.11.3 Frame Symbols in the Summary Pane 76
4.4.1.11.4 Decode Pane 76
4.4.1.11.5 Radix or Hexadecimal Pane 77
4.4.1.11.6 Character Pane 77
4.4.1.11.7 Binary Pane 78
4.4.1.11.8 Event Pane 78
4.4.1.11.9 Change Text Highlight Color 78

4.4.1.12 Protocol Layer Colors 79
4.4.1.12.1 Data Byte Color Notation 79
4.4.1.12.2 Changing Protocol Layer Colors 79
4.4.1.13 Filtering 79
4.4.1.13.1 Display Filters 80
4.4.1.13.1.5 Defining Node and Conversation Filters
4.4.1.13.1.6 The Difference Between Deleting and Hiding Display Filters
4.4.1.13.1.7 Editing Filters
4.4.1.13.2 Connection Filtering 89
4.4.1.13.2.1 Creating a Connection Filter
4.4.1.13.2.2 Connection Filter Display
4.4.1.13.3 Protocol Filtering from the Frame Display 94
4.4.1.13.3.1 Quick Filtering on a Protocol Layer
4.4.1.13.3.2 Easy Protocol Filtering
4.4.2 Coexistence View 95
4.4.2.1 Coexistence View Menus 96
4.4.2.2 Coexistence View - Toolbar 103
4.4.2.3 Coexistence View - Throughput Indicators 105
4.4.2.4 Throughput 105
4.4.2.5 Radio Buttons 106
4.4.2.6 All radio button 106
4.4.2.7 Selected radio button 106
4.4.2.8 Viewport radio button 106
4.4.2.9 Indicator width 107
4.4.2.10 Coexistence View - Throughput Graph 108
4.4.2.11 Throughput Graph Y-axis labels 108
4.4.2.12 Excluded packets 109
4.4.2.13 Tooltips 109
4.4.2.14 Discontinuities 109
4.4.2.15 Viewport 110
4.4.2.16 Swap button 111

4.4.2.17 Dots button 112
4.4.2.18 Zoomed Throughput Graph 113
4.4.2.19 Zoom Cursor 115
4.4.2.20 Comparison with the Bluetooth Timeline's Throughput Graph 115
4.4.2.21 Coexistence View - Set Button 116
4.4.2.22 Coexistence View - Throughput Radio Buttons 117
4.4.2.23 Coexistence View - Timeline Radio Buttons 117
4.4.2.24 Coexistence View – low energy Devices Radio Buttons 117
4.4.2.25 Coexistence View – Legend 118
4.4.2.26 Coexistence View – Timelines 118
4.4.2.27 Packet information 118
4.4.2.28 Relocating the tool tip 121
4.4.2.29 The two Timelines 123
4.4.2.30 Bluetooth slot markers 125
4.4.2.31 Zooming 125
4.4.2.32 Discontinuities 126
4.4.2.33 High-Speed Bluetooth 127
4.4.2.34 Coexistence View - No Packets Displayed with Missing Channel Numbers 128
4.4.2.35 High Speed Live View 129
4.5 Data/Audio Extraction 130
4.6 Statistics 133
4.6.1 Statistics Window 133
4.6.2 Session, Resettable and Capture File Tabs 136
4.6.3 Copying Statistics To The Clipboard 137
4.6.4 802.11 Error Statistics 137
4.6.5 Graphs 137
4.6.5.1 Statistics Errors Graphs 137
4.6.5.2 Printing Error Graphs 138
Chapter 5 Navigating and Searching the Data 139
5.1 Find 139
5.1.1 Searching within Decodes 140

5.1.2 Searching by Pattern 142
5.1.3 Searching by Time 144
5.1.4 Using Go To 146
5.1.5 Searching for Special Events 147
5.1.6 Searching by Signal 148
5.1.7 Searching for Data Errors 152
5.1.8 Find - Bookmarks 154
5.1.9 Changing Where the Search Lands 155
5.1.10 Subtleties of Timestamp Searching 156
5.2 Bookmarks 156
5.2.1 Adding, Modifying or Deleting a Bookmark 156
5.2.2 Displaying All and Moving Between Bookmarks 157
Chapter 6 Saving and Importing Data 159
6.1 Saving Your Data 159
6.1.1 Saving the Entire Capture File 159
6.1.2 Saving the Entire Capture File with Save Selection 160
6.1.3 Saving a Portion of a Capture File 161
6.2 Adding Comments to a Capture File 161
6.3 Confirm Capture File (CFA) Changes 162
6.4 Loading and Importing a Capture File 162
6.4.1 Loading a Capture File 162
6.4.2 Importing Capture Files 163
6.5 Printing 163
6.5.1 Printing from the Frame Display/HTML Export 163
6.5.2 Printing from the Event Display 166
6.6 Exporting 167
6.6.1 Frame Display Export 167
6.6.2 Exporting a File with Event Display Export 167
6.6.2.1 Export Filter Out 170
6.6.2.2 Exporting Baudot 170
Chapter 7 General Information 171

7.1 System Settings and Progam Options 171
7.1.1 System Settings 171
7.1.1.1 System Settings - Disabled/Enabled Options 173
7.1.1.2 Advanced System Options 173
7.1.1.3 Selecting Start Up Options 174
7.1.2 Changing Default File Locations 175
7.1.3 Side Names 177
7.1.4 Timestamping 178
7.1.4.1 Timestamping Options 178
7.1.4.2 Enabling/Disabling Timestamp 179
7.1.4.3 Changing the Timestamp Resolution 179
7.1.4.4 Switching Between Relative and Absolute Time 180
7.1.4.5 Displaying Fractions of a Second 181
7.2 Technical Information 181
7.2.1 Performance Notes 181
7.2.2 Ring Indicator 182
7.2.3 Progress Bars 182
7.2.4 Event Numbering 182
7.2.5 Useful Character Tables 182
7.2.5.1 ASCII Codes 183
7.2.5.2 Baudot Codes 183
7.2.5.3 EBCDIC Codes 184
7.2.5.4 Communication Control Characters 184
7.2.6 The Frontline Serial Driver 185
7.2.7 DecoderScript Overview 185
7.2.8 Bluetooth low energy ATT Decoder Handle Mapping 186
7.3 Contacting Technical Support 187
Appendicies 189
Appendix A: Application Notes 191
A.1 802.11 Conductive Testing-Isolating the Environment 193
A.1.1 Test Equipment 193

A.1.2 Test Setup - 802.11 193
A.1.3 Test Process 194
A.2 ComProbe Automation Server: Why use it? 195
A.2.1 Automation Server Topology 196
A.2.2 Writing Automation Script 196
A.2.3 Running Automation Server Script 198
A.2.4 Saving Automation Captured Data 201
A.2.5 Keeping Track of Events 203
A.2.6 Automation Can Save Time and Money 203

List of Figures

Figure 2.1 - Front Panel 4
Figure 2.2 - ComProbe 802.11 with both antennas attached 5
Figure 2.3 - Back Panel - Power 5
Figure 2.4 - Back Panel - USB 6
Figure 2.5 - Back Panel - ProbeSync with BPA 600 7
Figure 2.6 - Desktop Folder Link 8
Figure 2.7 - ComProbe Analyzer Control Window 11
Figure 3.1 - 802.11 Hardware Settings Dialog 18
Figure 3.2 - 802.11 I/O Settings Dialog 19
Figure 3.3 - 802.11 I/O Settings Settings Tab 20
Figure 3.4 - 802.11 I/O Settings Status Tab 21
Figure 3.5 - 802.11 I/O Settings Capture Filters Tab 22
Figure 3.6 - 802.11 I/O Settings Capture Filters Add New Address Dialog 22
Figure 3.7 - 802.11 I/O Settings Capture Filters Edit MAC Address Dialog 23
Figure 3.8 - 802.11 I/O Settings Firmware Update Tab 24
Figure 3.9 - 802.11 I/O Settings Firmware Update Version List 25
Figure 3.10 - 802.11 Device Scanner with no Devices Detected 25
Figure 3.11 - 802.11 Device Scanner with Devices Detected 26
Figure 3.12 - 802.11 Hardware Settings Dialog 27

Figure 3.13 - Wi-Fi Device Scanner I/O Settings Dialog 28
Figure 3.14 - Wi-Fi Direct MAC Address Editor 29
Figure 3.15 - Select Set Initial Decoder Parameters... from Control window 30
Figure 3.16 - Tabs for each decoder requiring parameters. 30
Figure 3.17 - Set Subsequent Decoder Parameters... from Control window 31
Figure 3.18 - Example: Set Subsequent Decode for Frame #52, RFCOMM 31
Figure 3.19 - Security (WPA2/WEP) Decoder Tab 33
Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane 38
Figure 4.2 - Example: Poor Capture Environment 39
Figure 4.3 - Packet Transfer Dialog 41
Figure 4.4 - Datasource Stopped Sniffing 41
Figure 4.5 - Datasource Sniffing 42
Figure 4.6 - Wireshark Capture Dialog 42
Figure 4.7 - Wi-Fi Datasource Toolbar 42
Figure 4.8 - Wi-Fi Datasource Sniffing Menu 43
Figure 4.9 - Wireshark Capture Options 43
Figure 4.10 - Incorrect ProbeSync Hardware Connection Error 45
Figure 4.11 - Incorrect ProbeSync Hardware Connection Message In Datasource Status 45
Figure 4.12 - ProbeSync Synchronizing Device Status Message 45
Figure 4.13 - ProbeSync Synchronized Device Status Message 45
Figure 4.14 - Frame Display Extended Inquire Response 46
Figure 4.15 - Format Menu 56
Figure 4.16 - Header labels, right click 57
Figure 4.17 - Data display right click menu 57
Figure 4.18 - Event Display Options menu 60
Figure 4.19 - Event Display Font Size Selection 60
Figure 4.20 - Frame Display with all panes active 61
Figure 4.21 - Frame Display Find text entry field 67
Figure 4.22 - Search/Find Dialog 68
Figure 4.23 - Frame Display File menu, Byte Export 71
Figure 4.24 - Byte Export dialog 71

Figure 4.25 - Save As dialog 72
Figure 4.26 - Sample Exported Frames Text File 72
Figure 4.27 - Example Protocol Tags 73
Figure 4.28 - Summary pane (right) with Tooltip on Column 5 (Tran ID) 74
Figure 4.29 - Frame Display Protocol Layer Color Selector 79
Figure 4.30 - Example: Set Conditions Self Configuring Based on Protocol Selection 81
Figure 4.31 - Example: Set Conditions Self Configuring Based on Frame Range 82
Figure 4.32 - Two Filter Conditions Added with an AND Operator 84
Figure 4.33 - Save Named Filter Condition Dialog 84
Figure 4.34 - Using Named Filters Section of Quick Filters to Show/Hide Filters 87
Figure 4.35 - Set Condition Dialog in Advanced View 88
Figure 4.36 - Rename Filters Dialog 89
Figure 4.37 - Connection Filter from the Frame Display Menu 90
Figure 4.38 - Connection Filter from the Frame Display Toolbar right-click 90
Figure 4.39 - Connection Filter from the Frame Display Pane right-click 91
Figure 4.40 - Connection Filter from frame selection right-click 92
Figure 4.41 - Front Display: Filtered on Access Address 0x8e89bed6 93
Figure 4.42 - Unfiltered: Capture File with Classic, low energy, and 802.11 94
Figure 4.43 - Connection Filter selecting All 802.11 frames, front 94
Figure 4.44 - Frame Display Quick Filtering and Hiding Protocols Dialog 95
Figure 4.45 - Coexistence View Window 96
Figure 4.46 - Coexistence View Toolbar 103
Figure 4.47 - Coexistence View Throughput Indicators 105
Figure 4.48 - Throughput Graph viewport. 107
Figure 4.49 - Average throughput indicators show a plus sign (+) when the indicator width is exceeded. 107
Figure 4.50 - A single selected packet 107
Figure 4.51 - Coexistence View Throughput Graph 108
Figure 4.52 - Throughput Graph y-axis labels. 109
Figure 4.53 - Data point tooltip 109
Figure 4.54 - A negative discontinuity. 110
Figure 4.55 - Three positive discontinuities. 110

Figure 4.56 - Throughput Graph Viewport 111
Figure 4.57 - Small Timeline and large Throughput Graph after pressing the Swap button. 112
Figure 4.58 - Dots Toggled On and Off 112
Figure 4.59 - Overlapping Dots Information Display 113
Figure 4.60 - Synchronized Zoomed Throughput Graph and View Port 114
Figure 4.61 - Zoomed Throughput Graph- Largest Value Snaps to Top 114
Figure 4.62 - Zoomed Throughput Graph - Freeze Y keeps the y-axis constant 115
Figure 4.63 - 802.11 Source Address Dialog 116
Figure 4.64 - 802.11 Source Address Drop Down Selector 117
Figure 4.65 - Coexistence View Legend 118
Figure 4.66 - Coexistence View Timelines 118
Figure 4.67 - Each packet is color-coded 119
Figure 4.68 - Highlighted entries in the legend for a selected packet. 119
Figure 4.69 - Timeline header for a single selected packet. 119
Figure 4.70 - Timeline header for multiple selected packets 120
Figure 4.71 - Descriptive text on timeline packets. 120
Figure 4.72 - A tool tip for a Classic Bluetooth packet. 121
Figure 4.73 - Coexistence View Format Menu - Show Tooltips on Computer Screen 122
Figure 4.74 - Coexistence View Timeline Tool Tip Shown Anchored to Computer Screen 123
Figure 4.75 - 5 GHz and 2.4 GHz 802.11 packets 124
Figure 4.76 - 5 GHz information window 125
Figure 4.77 - 2.4 GHz information windows 125
Figure 4.78 - Vertical blue lines are Bluetooth slot markers 125
Figure 4.79 - A negative discontinuity 126
Figure 4.80 - A positive discontinuity 127
Figure 4.81 - Timeline header with discontinuity 127
Figure 4.82 - Timeline duration footer with discontinuity 127
Figure 4.83 - High-speed Bluetooth packets have a blue frequency box and a two-tone tool tip 128
Figure 4.84 - Missing Channel Numbers Message in Timelines 128
Figure 4.85 - 802.11 Statistics Window 134
Figure 4.86 - 802.11 Edit Menu for Copying 137

Figure 5.1 - Find Dialog 139
Figure 5.2 - Find Decode Tab Search for String 140
Figure 5.3 - Find Decode Tab Side Restriction 141
Figure 5.4 - Find Pattern Tab 143
Figure 5.5 - Find Pattern Tab Side Restrictions 143
Figure 5.6 - Find by Time tab 144
Figure 5.7 - Find Go To tab 146
Figure 5.8 - Find Special Events tab 148
Figure 5.9 - Find Signal tab. 149
Figure 5.10 - Find Signal Tab 150
Figure 5.11 - Find Error tab. 152
Figure 5.12 - Find Bookmark tab. 155
Figure 5.13 - Bookmarked Frame (3) in the Frame Display 156
Figure 5.14 - Find Window Bookmark tab Used to Move Around With Bookmarks 158
Figure 6.1 - Windows Save dialog 160
Figure 6.2 - Frame Display Print Dialog 164
Figure 6.3 - Frame Display Print Preview Dialog 165
Figure 6.4 - Event Display Print Dialog 167
Figure 6.5 - Event Display Export Example: .csv file. 168
Figure 6.6 - Example: .csv Event Display Export, Excel spreadsheet 170
Figure 7.1 - System Settings Single File Mode 172
Figure 7.2 - Advanced System Options dialog 174
Figure 7.3 - Start Up Options dialog 175
Figure 7.4 - File Locations dialog 176
Figure 7.5 - File Locations Browse dialog 176
Figure 7.6 - Example: Side Names Where "Slave" and "Master" are current 178
Figure A.1 - ComProbe 802.11 Conductive Test Setup for 3X3 MIMO 194

Chapter 1 ComProbe Hardware & Software

Frontline Test Equipment ComProbe family of protocol analyzers work with the following technologies.

- Classic Bluetooth®
- *Bluetooth* low energy
- Dual Mode *Bluetooth* (simultaneous Classic and low energy)
- *Bluetooth* Coexistence with 802.11
- *Bluetooth* HCI (USB, SD, High Speed UART)
- NFC
- 802.11 (Wi-Fi)
- SD
- USB
- HSU (High Speed UART)

The ComProbe hardware interfaces with your computer that is running our robust software engine called the ComProbe Protocol Analysis System or ComProbe software. Whether you are sniffing the air or connecting directly to the chip Frontline analyzers use the same powerful ComProbe software to help you test, troubleshoot, and debug communications faster.

ComProbe software is an easy to use and powerful protocol analysis platform. Simply use the appropriate ComProbe hardware or write your own proprietary code to pump communication streams directly into the ComProbe software where they are decoded, decrypted, and analyzed. Within the ComProbe software you see packets, frames, events, coexistence, binary, hex, radix, statistics, errors, and much more.

This manual is a user guide that takes you from connecting and setting up the hardware through all of the ComProbe software functions for your ComProbe hardware. Should you have any questions contact the Frontline Technical Support Team.

1.1 What is in this manual

The ComProbe User Manual comprises the following seven chapters. The chapters are organized in the sequence you would normally follow to capture and analyze data: set up, configure, capture, analyze, save. You can read them from beginning to end to gain a complete understanding of how to use the ComProbe hardware and software or you can skip around if you only need a refresher on a particular topic. Use the Contents, Index, and Glossary to find the location of particular topics.

- **Chapter 1 ComProbe Hardware and Software**. This chapter will describe the minimum computer requirements and how to install the software.
- **Chapter 2 Getting Started**. Here we describe how to set up and connect the hardware, and how to apply power. This chapter also describes how to start the ComProbe software in Data Capture Methods. You will be introduced to the Control window that is the primary operating dialog in the ComProbe software.
- **Chapter 3 Configuration Settings**. The software and hardware is configured to capture data. Configuration settings may vary for a particular ComProbe analyzer depending on the technology and network being sniffed. There are topics on configuring protocol decoders used to disassemble packets into frames and events.
- **Chapter 4 Capturing and Analyzing Data**. This Chapter describes how to start a capture session and how to observe the captured packets, frames, layers and events.
- **Chapter 5 Navigating and Searching the Data**. Here you will find how to move through the data and how to isolate the data to specific events, often used for troubleshooting device design problems.
- **Chapter 6 Saving and Importing Data**. When a live capture is completed you may want to save the captured data for future analysis, or you may want to import a captured data set from another developer or for use in interoperability testing. This chapter will explain how to do this for various data file formats.
- **Chapter 7 General Information**. This chapter provides advanced system set up and configuration information, timestamping information, and general reference information such as ASCII, baudot, and EBCDIC codes. This chapter also provides information on how to contact Frontline's Technical Support team should you need assistance.

1.2 Computer Minimum System Requirements

Frontline supports the following computer systems configurations:

- Operating System: Windows 7 and 8
- USB Port: USB 2.0 High-Speed or USB 3.0 Super-Speed

The ComProbe software must operate on a computer with the following minimum characteristics.

- Processor: Core i5 processor at 2.7 GHz
- RAM: 4 GB
- Free Hard Disk Space: 20 GB

1.3 Software Installation

1.3.1 From CD:

Insert the ComProbe installer disc into your DVD drive. Click on the **Install CPAS** shortcut and follow the directions.

1.3.2 From Download:

Download the latest **CPAS installer** from FTE.com. Once downloaded, double-click the installer and follow the directions.

Chapter 2 Getting Started

In this chapter we introduce you to the ComProbe hardware and show how to start the ComProbe analyzer software and explain the basic software controls and features for conducting the protocol analysis.

2.1 802.11 Hardware

Attaching Antennas

When you remove the ComProbe 802.11 from the box, the first step is to attach the antennas (Figure 2.1).

Figure 2.1 - Front Panel

1. Attach an antenna to each front panel connector.

Figure 2.2 - ComProbe 802.11 with both antennas attached

2.1.1 Connecting/Powering the ComProbe 802.11

Once you have attached the antennas, the next step is to power up and connect the ComProbe 802.11 to the computer.

1. Insert the power cable (DC connector) from the 12 volt AC adapter into the **Power** port on the ComProbe 802.11 back panel (Figure 2.3).

Figure 2.3 - Back Panel - Power

2. Plug the 12 volt AC adapter into the AC power source. The front panel **Power** light illuminate (Figure 2.1).
3. Insert the USB cable into the **USB** port on the ComProbe 802.11 back panel (Figure 2.4).

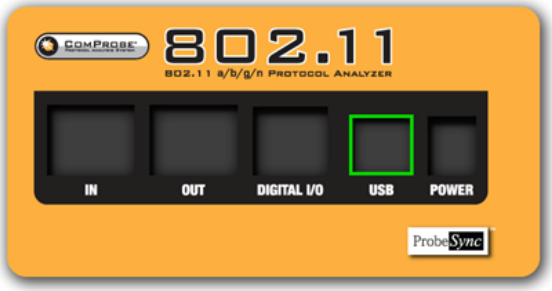


Figure 2.4 - Back Panel - USB

4. Insert the other end of the USB cable into the PC.
5. It may take as long as thirty seconds for Windows to recognize that the ComProbe 802.11 hardware is connected to the PC. The **Activity** light on the ComProbe 802.11 front panel (Figure 2.1 will blink during this period, when the light is steady, the ComProbe 802.11 hardware is ready to communicate with the ComProbe software.

2.1.2 Setting Up for ProbeSync™

The ComProbe 802.11 hardware has ProbeSync™ which allows for synchronization of ComProbe hardware clocks and timestamping. One ComProbe device will act as the master device by providing the clock to the slave device receiving the clock. Do not confuse "master" and "slave" with Bluetooth® device master and slave relationships. When using the ComProbe 802.11 with a ComProbe BPA 600 the BPA 600 must always be the master ProbeSync device. Refer to the following table.

Table 2.1 - 802.11 ProbeSync Relationships

Master	Slave
No. 1 ComProbe 802.11	No. 2 ComProbe 802.11
ComProbe BPA 600	ComProbe 802.11

1. Using a CAT 5 Ethernet cable (less than 1.5 meters (4.9 feet)) insert one end to the master ComProbe device OUT jack.
2. Insert the other end of the cable into the slave ComProbe device IN jack.

Note: The ComProbe BPA 600 device must always be the master node in ProbeSync mode.

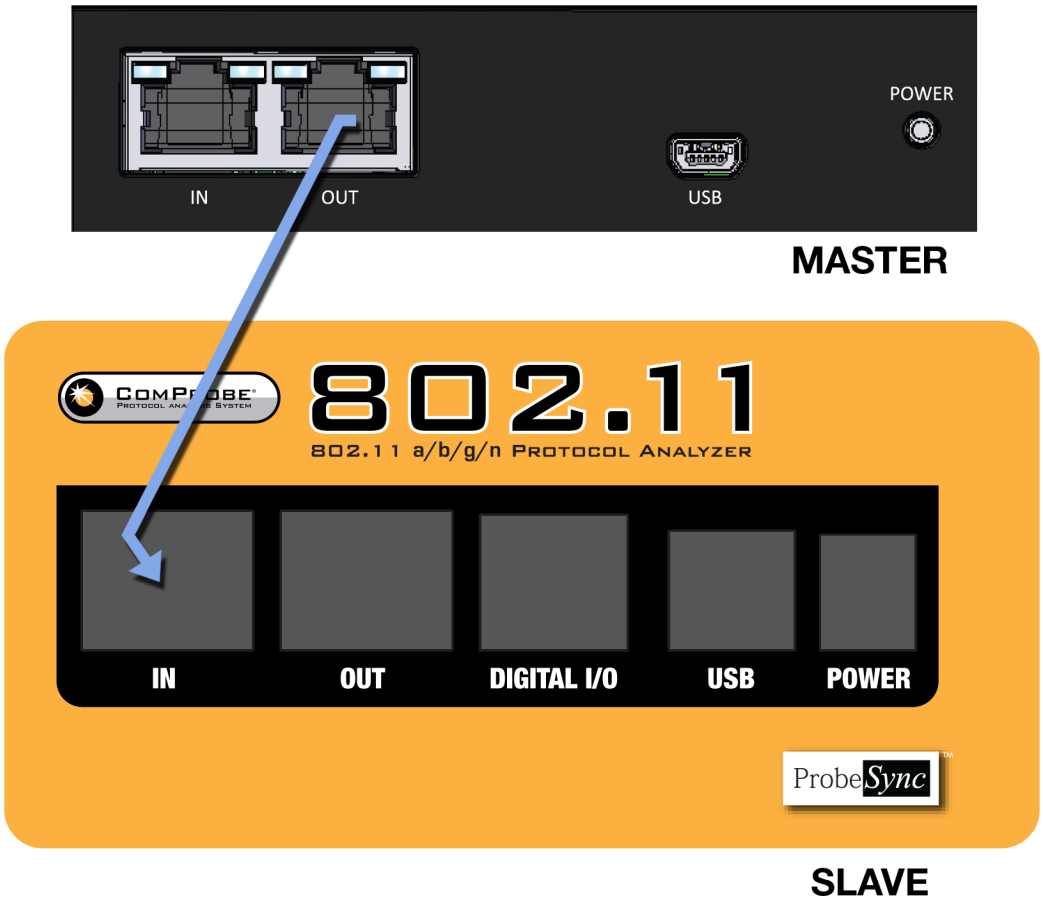


Figure 2.5 - Back Panel - ProbeSync with BPA 600

2.2 Data Capture Methods

This section describes how to load Frontline Test Equipment, Inc ComProbe Protocol Analysis System software, and how to select the data capture method for your specific application.

2.2.1 Opening ComProbe Data Capture Method

On product installation, the installer creates a folder on the windows desktop labeled "Frontline ComProbe Protocol Analysis System <version#>".

1. Double-click the "Frontline ComProbe Protocol Analysis System" desktop folder

This opens a standard Windows file folder window.

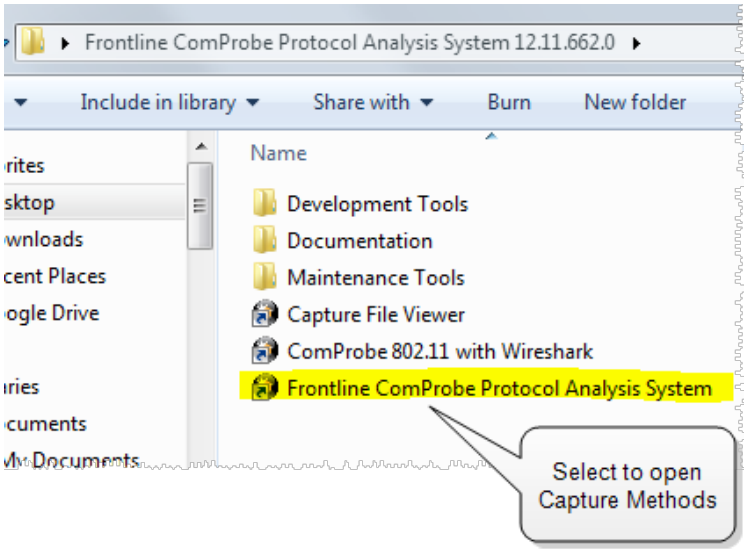


Figure 2.6 - Desktop Folder Link

2. Double-click on **Frontline ComProbe Protocol Analysis System** and the system displays the Select Data Capture Method dialog.

Note: You can also access this dialog by selecting Start > All Programs > Frontline ComProbe Protocol Analysis System (Version #) > Frontline ComProbe Protocol Analysis System

Three buttons appear at the bottom of the dialog; **Run**, **Cancel**, and **Help**. When the dialog first opens, Cancel and Help are active, and the Run button is inactive (grayed out).

Run starts the selected protocol stack.

Cancel closes the dialog and exits the user back to the desktop.

Help takes the user to this help file as does pressing the F1 key.

3. Expand the folder and select the data capture method that matches your configuration.
4. Click on the Run button and the ComProbe Control Window will open configured to the selected capture method.

Note: If you don't need to identify a capture method, then click the Run button to start the analyzer.

Creating a Shortcut

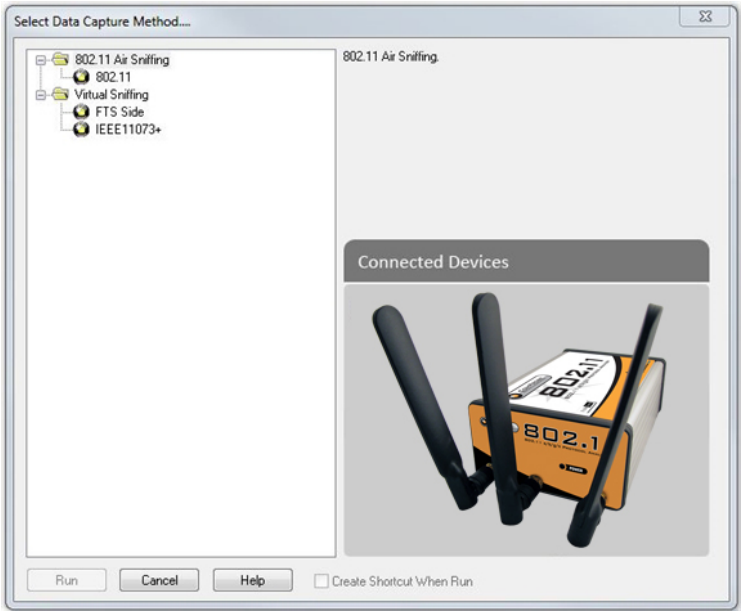
A checkbox labeled Create Shortcut When Run is located near the bottom of the dialog. This box is un-checked by default. Select this checkbox, and the system creates a shortcut for the selected method, and places it in the "Frontline ComProbe Protocol Analysis System <version#>" desktop folder and in the start menu when you click

the Run button. This function allows you the option to create a shortcut icon that can be placed on the desktop. In the future, simply double-click the shortcut to start the analyzer in the associated protocol.

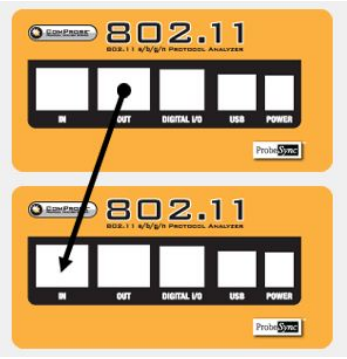
Supporting Documentation

The Frontline ComProbe Protocol Analysis System directory contains supporting documentation for development (Automation, DecoderScript, application notes), user documentation (Quick Start Guides and User Manual), and maintenance tools.

2.2.2 ComProbe 802.11 Air Sniffing Data Capture Methods



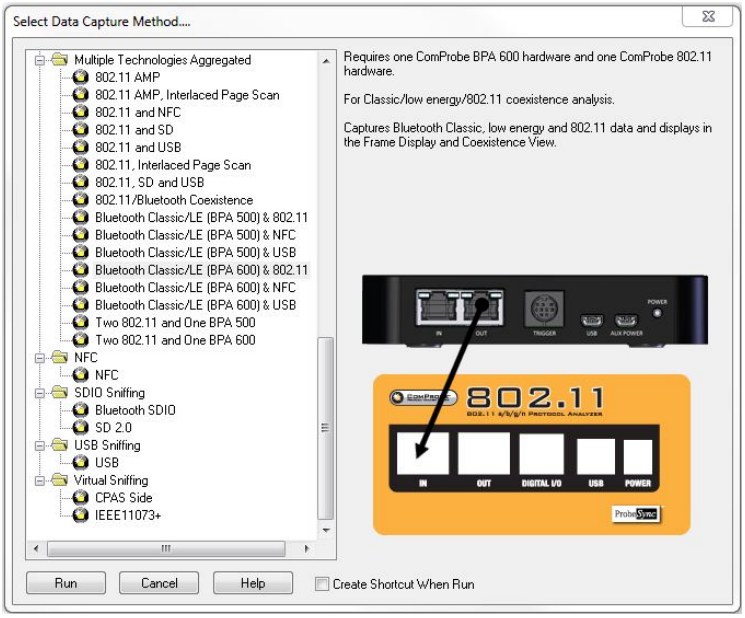
- 802.11
  - Requires one ComProbe 802.11 hardware.
  - Captures 802.11 data on the selected channel.
- 802.11 Double
  - Requires two ComProbe 802.11 hardware.



- 802.11 Triple
  - Requires three ComProbe 802.11 hardware.
- 802.11 with USB
  - Requires one ComProbe 802.11 and one ComProbe USB hardware.
- 802.11 with USB and SD
  - Requires one ComProbe 802.11, one ComProbe USB, and one ComProbe SD hardware.

2.2.3 Bluetooth® /802.11 Air Sniffing Multiple Technologies Aggregated.

ComProbe® Protocol Analysis System can capture Bluetooth and 802.11 simultaneously and display results in the **Coexistence View**.



- Requires one ComProbe BPA 600 hardware and one ComProbe 802.11 hardware.
- For *Bluetooth* Classic, Bluetooth low energy, and 802.11 coexistence analysis.

2.2.4 Virtual Sniffing

The Virtual Sniffer is a live import facility within ComProbe software that makes it possible to access any layer in a stack that the programmer has access to and feed this data into the Virtual Sniffer. Please refer to the “Show Live Import Information“ button on the Virtual Sniffer Datasource window in ComProbe software. More information is available in the Live Import Developer's Kit located in the Development Tools folder in Frontline ComProbe Protocol Analysis System desktop folder, and a white paper is available at Bluetooth Virtual Sniffing

- **FTS Side**
  - No hardware required.
  - ComProbe software acquires data via user-developed software.

- **IEEE 11073+**
  - No hardware required
  - for sniffing data virtually from the continua Enabling Software Library (CESL) IEEE 11073 tester.

2.2.5 Determining Master and Slave

In Bluetooth® , the device that initiates the connection is always the master at connection time. You only need to know the master and slave at connection time when setting up the I/O Settings. Afterward a role switch may occur, but the analyzer automatically follows the role switch.

Note: You do not have to identify a Master address if you are using Firmware Version 62 or newer.

Role Switches

After the connection has been made, a role switch can take place. A good example of why this happens would be when a mouse connects to the PC. The mouse initiates the connection, so it is the master. After the connection is made, a role switch occurs so that the PC becomes the master and the mouse becomes a slave. The role switch takes place because the PC may be working with multiple devices at the same time, and as such, the PC would not be a slave of more than one device.

Let us say that a link exists between a PC and a keyboard with the PC a master. If the mouse wants to become a member of the link it initiates the connection. Since the mouse initiated the connection, it is the master of a new link and the PC is the slave. The PC is still the master of the link between the PC and keyboard. A role switch now occurs between the PC and the mouse, and the PC is now the master of a link with two slaves: the mouse and keyboard.

2.3 Control Window

The analyzer displays information in multiple windows, with each window presenting a different type of information. The Control window opens when the **Run** button is clicked in the **Select Data Capture Method** window. The Control window provides access to each ComProbe analyzer functions and settings as well as a brief overview of the data in the capture file. Each icon on the toolbar represents a different data analysis function. A sample Control Window is shown below.

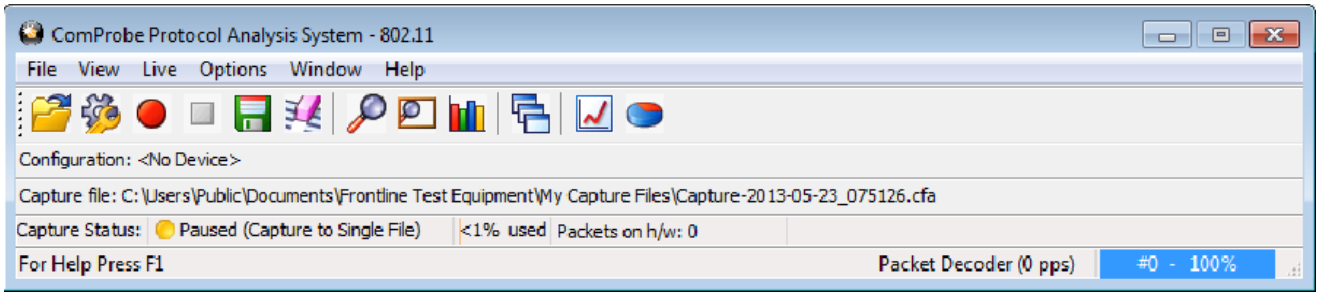

ComProbe Protocol Analysis System - 802.11
File View Live Options Window Help
Configuration: <No Device>
Capture file: C:\Users\Public\Documents\Frontline Test Equipment\My Capture Files\Capture-2013-05-23_075126.cfa
Capture Status: Paused (Capture to Single File)
<1% used
Packets on h/w: 0
For Help Press F1
Packet Decoder (0 pps)
#0 - 100%

Figure 2.7 - ComProbe Analyzer Control Window

Because the **Control** window can get lost behind other windows, every window has a **Home** icon that brings the Control window back to the front. Just click on the Home icon to restore the **Control** window.

When running the Capture File Viewer, the Control window toolbar and menus contain only those selections needed to open a capture file and display the About box. Once a capture file is opened, the analyzer limits Control window functions to those that are useful for analyzing data contained in the current file. Because you cannot capture data while using Capture File Viewer, data capture functions are unavailable. For example, when viewing Ethernet data, the Signal Display is not available. The title bar of the Control window displays the name of the currently open file. The status line (below the toolbar) shows the configuration settings that were in use when the capture file was created.

2.3.1 Control Window Toolbar

Toolbar icon displays vary according to operating mode and/or data displayed. Available icons appear in color, while unavailable icons are not visible. Grayed-out icons are available for the ComProbe hardware and software configuration in use but are not active until certain operating conditions occur. All toolbar icons have corresponding menu bar items or options.

Table 2.2 - Control Window Toolbar Icon List

Icon	Description
	Open File - Opens a capture file.
	I/O Settings - Opens settings
	Start Capture - Begins data capture to disk
	Stop Capture - Available after data capture has started. Click to stop data capture. Data can be reviewed and saved, but no new data can be captured.
	Save - Saves the capture file.
	Clear - Clears or saves the capture file.
	Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.
	Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.
	Notes - Opens the Notes dialog.
	Cascade - Arranges windows in a cascaded display.
	Coexistence View - Opens the Coexistence View dialog.
	Wi-Fi Error Statistics - Opens the Wi-Fi Error Statistics dialog.

2.3.2 Configuration Information on the Control Window

The Configuration bar (just below the toolbar) displays the hardware configuration and may include I/O settings. It also provides such things as name of the network card, address information, ports in use, etc.

2.3.3 Status Information on the Control Window

The Status bar located just below the Configuration bar on the **Control** window provides a quick look at current activity in the analyzer.

- Capture Status, or Status for Sodera, displays Not Active, Paused or Running and refers to the state of data capture
    - Not Active means that the analyzer is not currently capturing data.
    - Paused means that data capture has been suspended.
    - Running means that the analyzer is actively capturing data.
- % Used

    The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 200 Kb capture file, the bar graph tells you how much of the capture file has been used. When the graph reaches 100%, capture either stops or the file begins to overwrite the oldest data, depending on the choices you made in the System Settings.
- Utilization/Events

    The second half of the status bar gives the current utilization and total number of events seen on the network. This is the total number of events monitored, not the total number of events captured. The analyzer is always monitoring the circuit, even when data is not actively being captured. These graphs allow you to keep an eye on what is happening on the circuit, without requiring you to capture data.

2.3.4 Frame Information on the Control Window

Frame Decoder information is located just below the Status bar on the Control window. It displays two pieces of information.

- Frame Decoder (233 fps) displays the number of frames per second being decoded. You can toggle this display on/off with Ctrl-D, but it is available only during a live capture.
- #132911 displays the total frames decoded.
- 100% displays the percentage of buffer space used.

2.3.5 Control Window Menus

The menus appearing on the **Control** window vary depending on whether the data is being captured live or whether you are looking at a .cfa file. The following tables describe each menu.

Table 2.3 - Control Window **File** Menu Selections

Mode	Selection	Hot Key	Description
Live	**Close**		Closes Live mode.
Capture File	**Go Live**		Returns to Live mode
	Reframe		If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you need to reframe in order for the protocol decode to be correct. See Reframing on page 49
	Unframe		Removes start-of-frame and end-of-frame markers from your data. SeeUnframing on page 49
	Recreate Companion File		This option is available when you are working with decoders. If you change a decoder while working with data, you can recreate the ".frm file", the companion file to the ".cfa file". Recreating the ".frm file" helps ensure that the decoders will work properly.
	Reload Decoders		The plug-ins are reset and received frames are decoded again.
Live & Capture File	**Open Capture File**	Ctrl--O	Opens a Windows Open file dialog. at the default location "...\Public Documents\Frontline Test Equipment\My Capture Files\". Capture files have a .cfa extension.
	Save	Ctrl-S	Saves the current capture or capture file. Opens a Windows Save As dialog at the default location "...\Public Documents\Frontline Test Equipment\My Capture Files\".
	Exit ComProbe Protocol Analysis System		Shuts down the ComProbe Protocol Analysis System and all open system windows.
	Recent capture files		A list of recently opened capture files will appear.

The **View** menu selections will vary depending on the ComProbe analyzer in use.

Table 2.4 - Control Window **View** Menu Selections

Mode	Selection	Hot key	Description
Live & Capture File	**Event Display**	Ctrl-Shift-E	Opens the Event Display window for analyzing byte level data.
	Frame Display	Ctrl-Shift-M	Opens the Frame Display window for analyzing protocol level data
	Statistics	Ctrl-Shift-S	Opens the Statistics Window that shows information about packet throughput.
	Coexistence View		Opens the Coexistence View window that can simultaneously display Classic *Bluetooth*, *Bluetooth* low energy, and 802.11 packets and thourghput.
	Wi-Fi Error Statistics		Opens the Wi-Fi Error Statistics window that displays the number of packet errors.

Table 2.5 - Control Window **Edit** Menu Selections

Mode	Selection	Hot-key	Description
Capture File	**Notes**	Ctrl-Shift-O	Opens the Notes window that allows the user to add comments to a capture file.

Control Window **Live** Menu Selections

Mode	Selection	Hot-Key	Description
Live	**Start Capture**	Shift-F5	Begins data capture from the configured wireless devices.
	Stop Capture	F10	Stops data capture from the configured wireless devices.
	Clear	Shift-F10	Clears or saves the capture file.

Table 2.6 - Control Window **Options** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Hardware Settings**		0 - Classic 1 - *Bluetooth* low energy
	I/O Settings		0 - Classic 1 - *Bluetooth* low energy
	System Settings	Alt-Enter	Opens the System Settings dialog for configuring capture files.
	Directories...		Opens the File Locations dialog where the user can change the default file locations.
	Check for New Releases at Startup		When this selection is enabled, the program automatically checks for the latest Frontline protocol analyzer software releases.
	Side Names...		Opens the Side Names dialog used to customize the names of the slave and master wireless devices.
	Protocol Stack...		Opens the Select a Stack dialog where the user defines the protocol stack they want the analyzer to use when decoding frames.
	Set Initial Decoder Parameters...		Opens the Set Initial Decoder Parameters window. Each entry in the window takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog. This selection is not present if no decoder is loaded that supports this feature.
	Set Subsequent Decoder Parameters...		Opens the Set Subsequent Decoder Parameters dialog where the user can override an existing parameter at any frame in the capture. Each entry takes effect from the specified frame onward or until redefined in this dialog on a later frame. This selection is not present if no decoder is loaded that supports this feature.
	Automatically Request Missing Decoder Information		When checked, this selection opens a dialog that asking for missing frame information. When unchecked, the analyzer decodes each frame until it cannot go further and it stops decoding. This selection is not present if no decoder is loaded that supports this feature.
	Enable/Disable Audio Expert System		When enabled, the Audio Expert System is active, other wise it is not available. Only available when an Audio Expert System licensed device is connected.

The **Windows** menu selection applies only to the **Control** window and open analysis windows: **Frame Display**, **Event Display**, **Message Sequence Chart**, **Bluetooth Timeline**, **Bluetooth low energy Timeline**, and **Coexistence View**. All other windows, such as the datasource, are not affected by these selections.

Table 2.7 - Control Window **Windows** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Cascade**	Ctrl-W	Arranges open analysis windows in a cascaded view with window captions visible.
	Close All Views		Closes Open analysis windows.
	Minimize Control Minimizes All		When checked, minimizing the Control window also minimizes all open analysis windows.
	Frame Display and **Event Display**		When these windows are open the menu will display these selections. Clicking on the selection will bring that window to the front.

Control Window **Help** Menu Selections

Mode	Selection	Hot-Key	Description
Live & Capture File	**Help Topics**		Opens the ComProbe Help window.
	About ComProbe Protocol Analysis System		Provides a pop-up showing the version and release information, Frontline contact information, and copyright information.
	Support on the Web		Opens a browser to fte.com technical support page.

2.3.6 Minimizing Windows

Windows can be minimized individually or as a group when the **Control** window is minimized. To minimize windows as a group:

1. Go to the **Window** menu on the **Control** window.
2. Select **Minimize Control Minimizes All**. The analyzer puts a check next to the menu item, indicating that when the **Control** window is minimized, all windows are minimized.
3. Select the menu item again to deactivate this feature.
4. The windows minimize to the top of the operating system Task Bar.

Chapter 3 Configuration Settings

In this section the ComProbe software is used to configure an analyzer for capturing data .

3.1 802.11 Configuration

3.1.1 ComProbe 802.11 Hardware Settings

The Hardware Settings dialog provides the ability to select a device to sniff/scan. The dialog only lists devices with a MAC address that match the Frontline devices. To access the Hardware Settings dialog:

1. Select Hardware Settings from the Options menu on the 802.11 Control window.

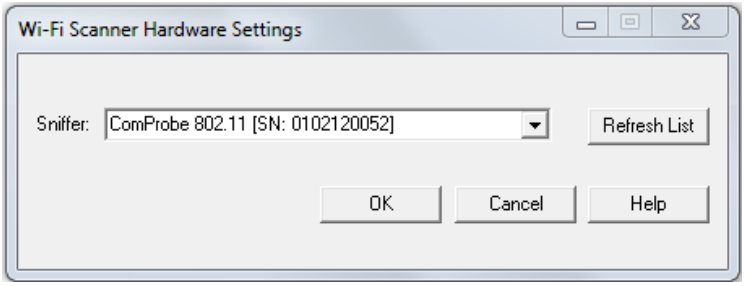


Figure 3.1 - 802.11 Hardware Settings Dialog

2. Select a device from the drop-down list.
3. Select OK

If no devices are found, the list is blank.

Note: Upon launching the Air Sniffer, the first device in the drop-down is the default device.

3.1.2 802.11 I/O Settings

1. Select **I/O Settings** from the **Options** menu on the **Control** window.

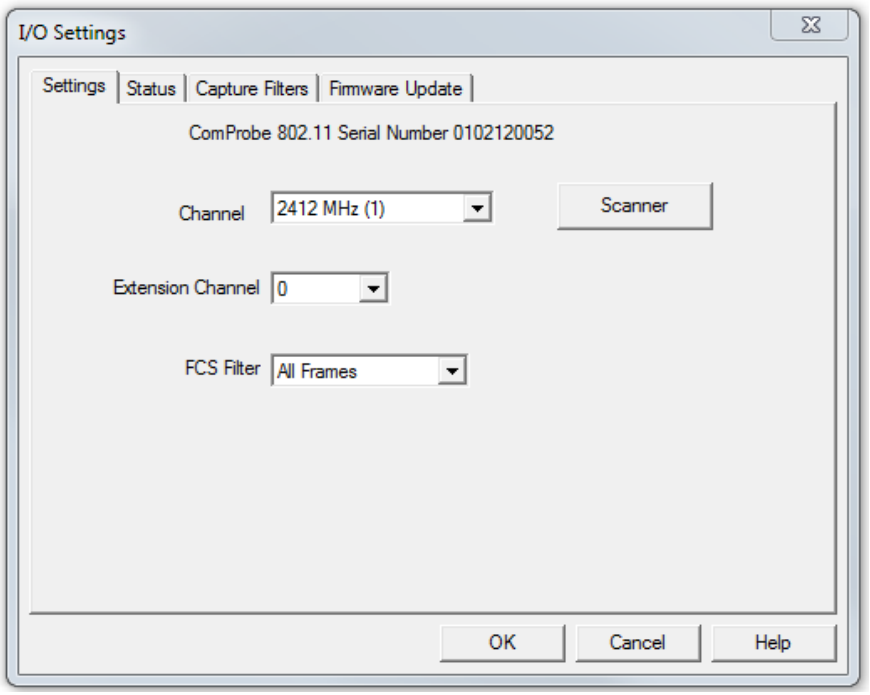


Figure 3.2 - 802.11 I/O Settings Dialog

There are several things to remember about **I/O Settings**:

- The **I/O Settings** are specific to the device selected in the **Hardware Settings**.
- Two 802.11 devices attached to a computer have different settings.
- Changing the settings changes the devices' default settings.
- If a parameter is changed (e.g. Channel 1 is changed to 6), the new setting appears the next time the **I/O Settings** dialog is opened for the device.
- The settings are saved when the **OK** button is pressed.

3.1.2.1 Settings

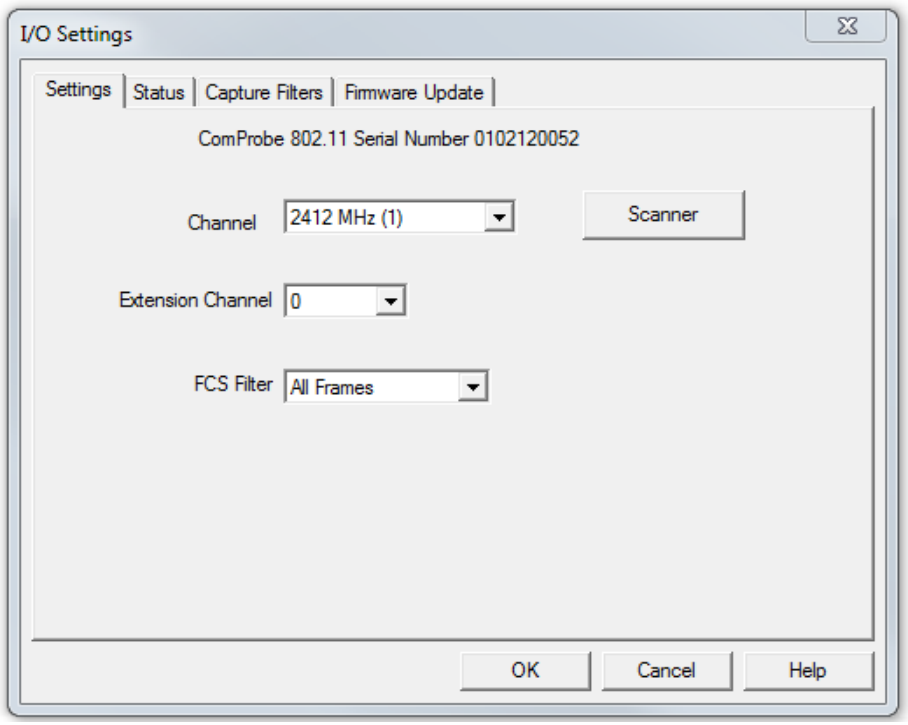


Figure 3.3 - 802.11 I/O Settings Settings Tab

The Settings dialog allows you to change and observe basic configuration values. These include the **Channel**, **Extension Channel**, **FCS Filter** and **Capture Type**.

- **Channel** - Select the channel from the drop-down list. Channels have been extended to the 5Ghz range.
- **Extension**- allows you to extend the range of channels available
  - 0 = Standard 1-14 Wi-Fi channels
  - -1 = Expanded channels below the standard range
  - +1 = Expanded channels above the standard range
- **FCS Filter** - The Frame Check Sequence filter indicates if the device should capture frames with an invalid FCS. Select **All Frames** or **Valid Frames**

Clicking on the **Scanner** button will open the **Wi-Fi Scanner** dialog. This action is useful if you do not know the channel to sniff. Once you have selected a channel in the **Wi-Fi Scanner** dialog and confirmed your selection the selected channel will appear in **Channel**.

3.1.2.2 Status

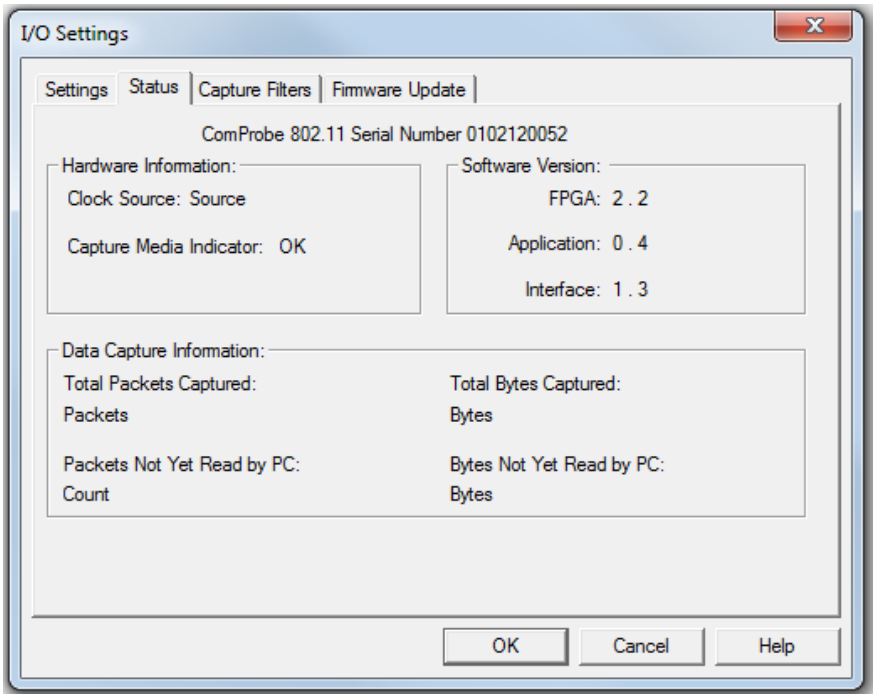


Figure 3.4 - 802.11 I/O Settings Status Tab

The Status dialog provides current information about the ComProbe device. There are no settings for this dialog.

3.1.2.3 Capture Filters

The **Capture Filters** dialog allows you create, modify, and delete capture filters. The dialog initially displays the existing MAC address Capture Filters.

- To activate the capture filters and to be able to create/modify additional filters, you first must select the **Enable MAC Address Capture Filters** check box.
- You can select/deselect which filters are active by checking/unchecking the **Enable** checkbox in the first column in the table.
- You can also select to ignore **Management**, **Control**, **Data**, and **Reserved** frame types by selecting one or more the checkboxes.

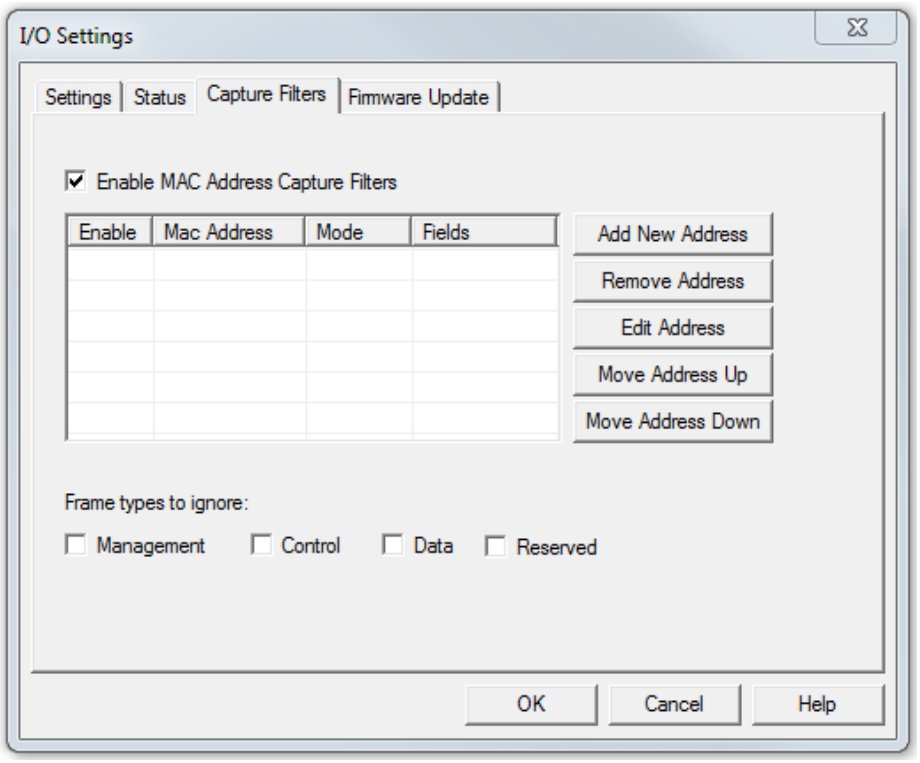


Figure 3.5 - 802.11 I/O Settings Capture Filters Tab

To create a key, select one of the following options:

- **Add New Address** - displays a text box where you can enter the address

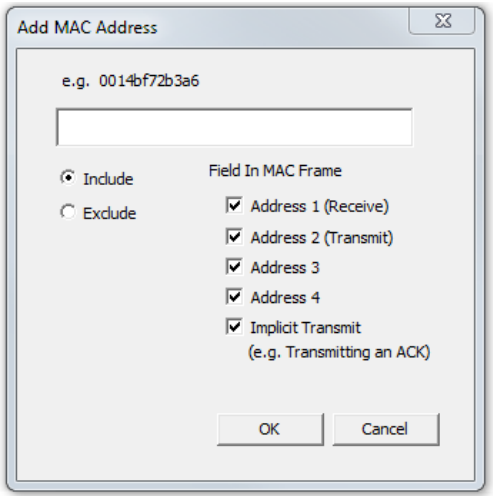


Figure 3.6 - 802.11 I/O Settings Capture Filters Add New Address Dialog

1. Enter a MAC Address in the text field.
2. Select the **Include** radio button to only capture packets with this MAC address.

3. Select the **Exclude** radio button to capture packets with other filters, but not ones with this MAC address.
4. Select one or more check boxes to identify which fields in the MAC Frame to include.

   The MAC header for an 802.11 frame can contain up to 4 address fields. Most frames do not have that many. In general, the first address is the intended receiver and the second address is the device that transmits the frame. The third and fourth address fields depend on the context of the frame. Some of the control type frames do not include the transmitter address but they may be determined from previous frames.
5. Select **OK** to close the dialog.

Once you have MAC addresses on the main dialog, you can modify them using four options.

- **Remove Address** - Highlight an address that you want to delete and select Remove Address to remove it from the list.
- **Edit Address** - Highlight an address that you want to edit and select Edit to bring up a dialog where you can edit the address. The address and any of the prior settings may be changes. Click **OK** to save and close.

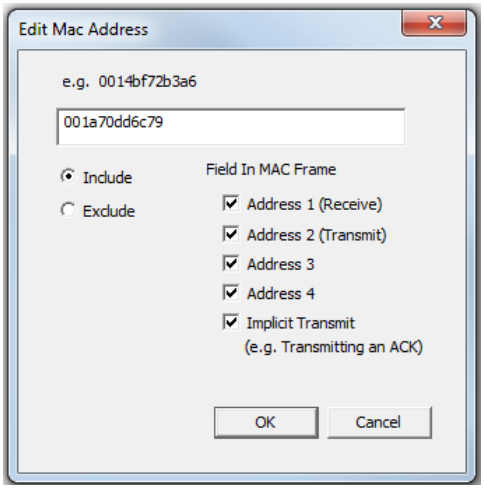


Figure 3.7 - 802.11 I/O Settings Capture Filters Edit MAC Address Dialog

- **Move Address Up** - moves the selected address up in the queue.
- **Move Address Down** - moves the selected address down in the queue.

3.1.2.4 Firmware Update

This tab displays the current firmware version in the hardware. You can check for the firmware updates by first noting the current version and then clicking on the **Check For Updates** button.

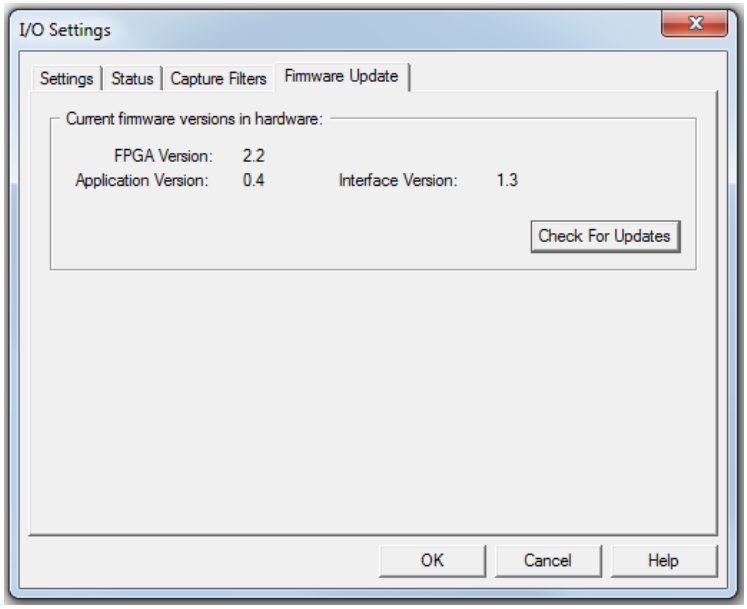


Figure 3.8 - 802.11 I/O Settings Firmware Update Tab

The **Check for Updates** dialog will open. If an update is available you can install it by clicking on the **Start Update** button.

The update process will begin and when finished the dialog will show a list of all completed actions. Upon completion of the update you will be notified of successful installation and returned to the **Firmware Update** dialog.

The **I/O Settings** dialog **Firmware** tab will open and show the old firmware version. At this point, the ComProbe 802.11 is rebooting. You will notice the **Activity** LED blinking on the ComProbe hardware. Click **OK** on the **I/O Settings** dialog.

An error message will appear. Ignore the message and click on the **Cancel** button. Completely exit the ComProbe software by selecting **Exit the ComProbe Protocol Analysis System** from the **Control** window **File** menu.

Wait for a solid **Activity** LED on the ComProbe hardware .

Important: Remove power from the ComProbe 802.11 hardware, and reapply power. Wait until the **Activity** LED comes back on and resume normal ComProbe operation.

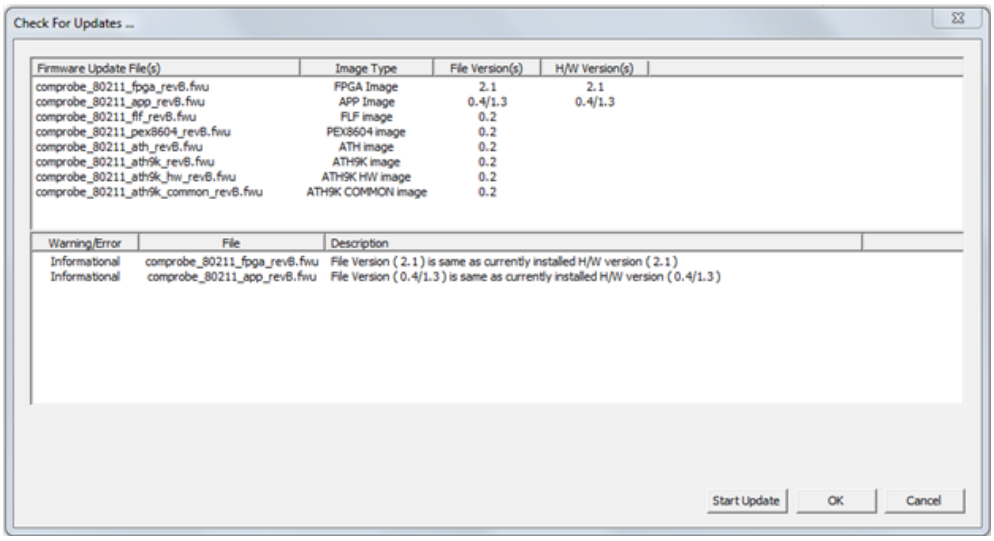


Figure 3.9 - 802.11 I/O Settings Firmware Update Version List

3.1.2.5 Security

Wi-Fi security settings are discussed in detail in the Decoder Parameters section .

3.1.2.6 Wi-Fi Device Scanner

1. On the **I/O Settings** dialog click on the **Settings** tab, and then click on the Scanner button. The **Wi-Fi Device Scanner** dialog will open.

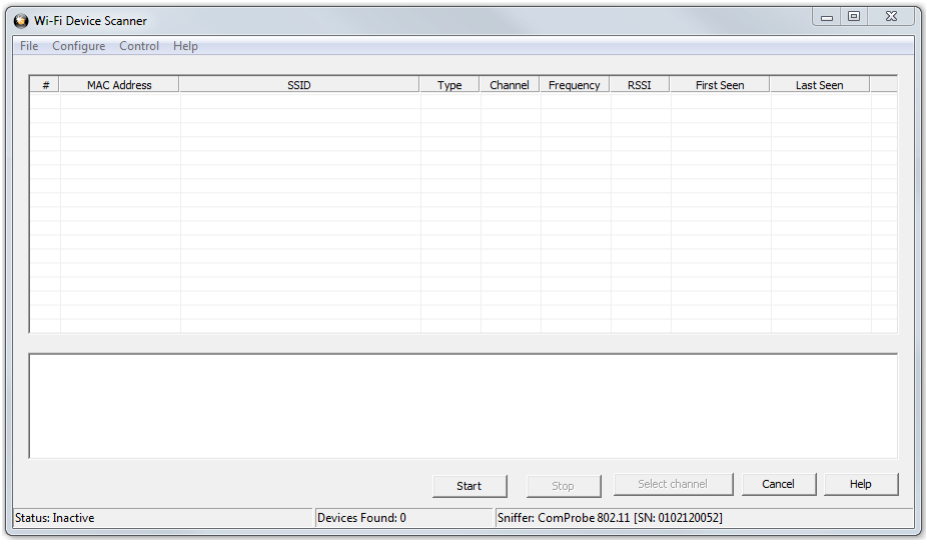


Figure 3.10 - 802.11 Device Scanner with no Devices Detected

2. On the **Wi-Fi Device Scanner** dialog Select the **Start** button or select **Start Scanning** from the **Control** menu to begin populating the list .

   The **Wi-Fi Device Scanner** dialog displays a list of discoverable Wi-Fi devices in a table. The devices are identified by:

- MAC Address
- SSID
- Type
- Channel
- Frequency
- RSSI
- First Seen
- Last Seen

Note: You can select the **Stop** or **Stop Scanning** from the **Configure** menu anytime to stop the device search.

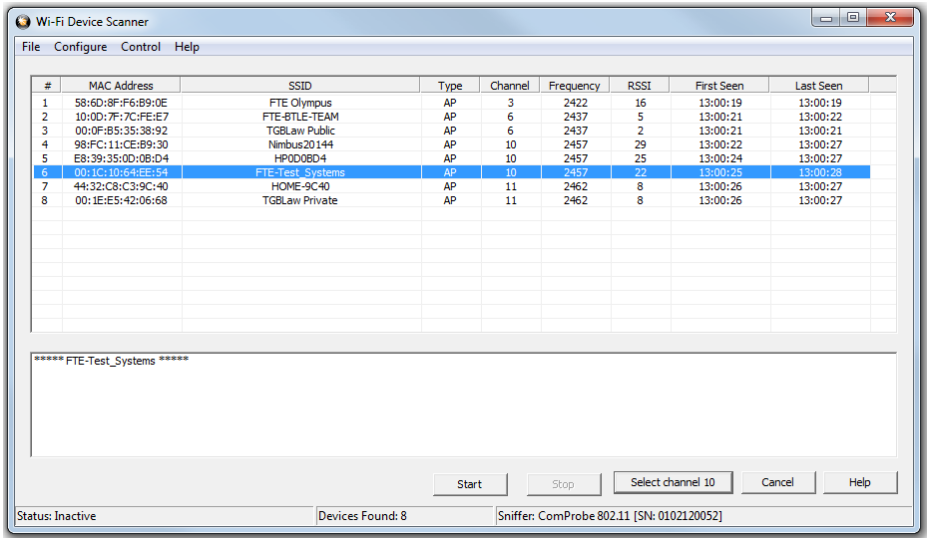
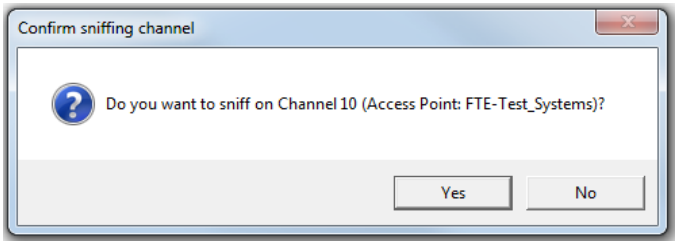

Wi-Fi Device Scanner
File Configure Control Help
MAC Address SSID Type Channel Frequency RSSI First Seen Last Seen
1 58:6D:8F:F6:B9:0E FTE Olympus AP 3 2422 16 13:00:19 13:00:19
2 10:0D:7F:7C:FE:E7 FTE-BTLE-TEAM AP 6 2437 5 13:00:21 13:00:22
3 00:0F:B5:35:38:92 TGBLaw Public AP 6 2437 2 13:00:21 13:00:21
4 98:FC:11:CE:B9:30 Nimbus20144 AP 10 2457 29 13:00:22 13:00:27
5 E8:39:35:0D:0B:D4 HP0D0BD4 AP 10 2457 25 13:00:24 13:00:27
6 00:1C:10:64:EE:54 FTE-Test_Systems AP 10 2457 22 13:00:25 13:00:28
7 44:32:C8:C3:9C:40 HOME-9C40 AP 11 2462 8 13:00:26 13:00:27
8 00:1E:E5:42:06:68 TGBLaw Private AP 11 2462 8 13:00:26 13:00:27
***** FTE-Test_Systems *****
Start Stop Select channel 10 Cancel Help
Status: Inactive
Devices Found: 8
Sniffer: ComProbe 802.11 [SN: 0102120052]

Figure 3.11 - 802.11 Device Scanner with Devices Detected

3. Select the device.
4. Click on **Select channel <*no*>**, where <*no*> is the channel number selected. The **Confirm Sniffing Channel** confirmation will appear. Click on **Yes** will close the **Wi-Fi Device Scanner** and the ComProbe analyzer will used the selected channel.



3.1.2.6.1 File Menu

Under the File menu you can select **Export to file** which converts the information in the table to a text file.

1. Select **Export to CSV file**. The **Save As** menu appears
2. Select where you want to save the file in **Save in**.
3. Enter a **File Name**.
4. Select **Save**.

3.1.2.6.2 Configure

From the Configure menu you can select , ,**Hardware Settings** and **I/O Settings**

3.1.2.6.3 ComProbe 802.11 Hardware Settings

The Hardware Settings dialog provides the ability to select a device to sniff/scan. The dialog only lists devices with a MAC address that match the Frontline devices. To access the Hardware Settings dialog:

1. Select Hardware Settings from the Options menu on the 802.11 Control window.

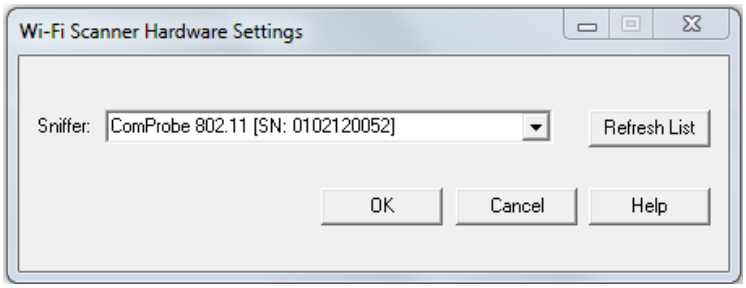


Figure 3.12 - 802.11 Hardware Settings Dialog

2. Select a device from the drop-down list.
3. Select OK

If no devices are found, the list is blank.

Note: Upon launching the Air Sniffer, the first device in the drop-down is the default device.

3.1.2.6.4 Wi-Fi Device Scanner - I/O Settings

The Device Scanner I/O Settings dialog is used to set a listening time and to activate a probe request. To access the I/O Settings dialog:

1. Select **I/O Settings** from the Configure menu on the Wi-Fi Device Scanner window.

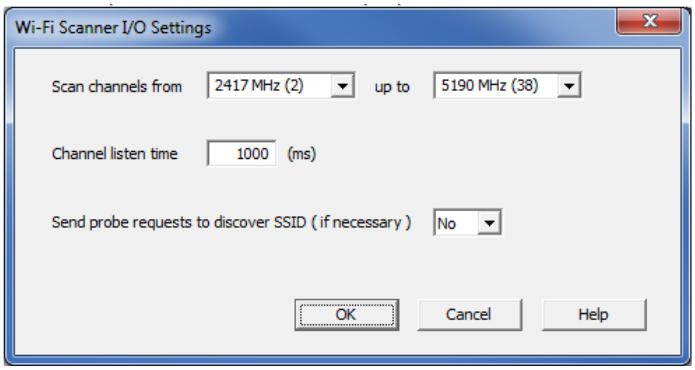


Figure 3.13 - Wi-Fi Device Scanner I/O Settings Dialog

2. **Scan Channels from**: Pick a lower and upper limit to scan a specific subset of frequencies. By default all channels are selected. Choosing a subset of frequencies to scan saves time and can be used when the user is interested in scanning only a certain range of frequencies.

3. Enter an amount, in msecs, for **Channel listen time**.

   Channel listen time is how long ComProbe 802.11 will listen on a channel to discover devices before moving on to the next channel.

4. Select **Yes** or **No** to choose whether to send a probe sync request.

   Sometimes an Access Point will intentionally not send it's SSID in a beacon to conceal it's identity. Selecting **Yes** for this option will send the MAC address, the SSID will be part of the Probe Response it sends back.

5. Select **OK** to save the options and close the dialog or **Cancel** to close the dialog without saving your choices.

3.1.2.6.5 Device Scanner RSSI Values

The 802.11 specification does not provide a relationship between the RSSI value and the actual power value. Here are the definitions from the specification.

1. RSSI in FHSS PHY: The RSSI is an optional parameter that has a value of 0 through RSSI Max. This parameter is a measure by the PHY of the energy observed at the antenna used to receive the current PPDU. RSSI shall be measured between the beginning of the SFD and the end of the PLCP HEC. RSSI is intended to be used in a relative manner. Absolute accuracy of the RSSI reading is not specified.

2. RSSI in DSSS PHY: The RSSI shall be a measure of the RF energy received by the DSSS PHY. RSSI indications of up to 8 bits (256 levels) are supported.

3. RSSI in OFDM PHY: The allowed values for the RSSI parameter are in the range from 0 through RSSI maximum. This parameter is a measure by the PHY of the energy observed at the antenna used to receive the current PPDU. RSSI shall be measured during the reception of the PLCP preamble. RSSI is intended to be used in a relative manner, and it shall be a monotonically increasing function of the received power.

Different vendors implement these value in their own way. The ComProbe 802.11 uses an Atheros chipset which provides RSSI values in the range of 0 to 128. The radio hardware in the ComProbe 802.11 has two receive chains (one for each antenna). Each received packet has RSSI values for both antennas as well as the combined value.

The hardware provides the following five values:

1. rssi_ant00: Receive signal strength indicator of control channel chain 0.
2. rssi_ant01: Receive signal strength indicator of control channel chain 1.
3. rssi_ant10: Receive signal strength indicator of extension channel chain 0.
4. rssi_ant11: Receive signal strength indicator of extension channel chain 1
5. rssi_combined: Receive signal strenth indicator of combination of all active chains on the control and extension channels.

All five of these values are shown in the PHY layer decoder for every packet. The Wi-Fi scanner shows the combined value.

3.1.3 Wi-Fi Device - MAC Address Editor

If you know the MAC Address of the device you can enter it manually.

1. From the I/O Settings dialog select the "Edit" button.
2. On the MAC Address Editor enter the MAC Address for the device.

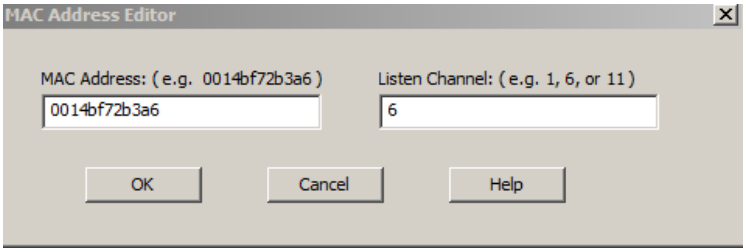


Figure 3.14 - Wi-Fi Direct MAC Address Editor

3. Enter a channel number in Listen Channel.
4. Select "OK".

The MAC Address appears on the I/O Settings dialog.

Once you close the dialog, the last MAC Address shown will appear when you reopen the dialog.

3.2 Decoder Parameters

Some protocol decoders have user-defined parameters. These are protocols where some information cannot be discovered by looking at the data and must be entered by the user in order for the decoder to correctly decode the data. For example, such information might be a field where the length is either 3 or 4 bytes, and which length is being used is a system option.

There may be times when the context for decoding a frame is missing. For example, if the analyzer captures a response frame but does not capture the command frame, then the decode for the response may be incomplete. The **Set Initial Decoder Parameters** window allows you to supply the context for any frame. The dialog allows you to define any number of parameters and save them in a template for later use

The decoder template function provides the capacity to create multiple templates that contain different parameters. This capability allows you to maintain individual templates for each Bluetooth® network monitored.

Applying a template containing only those parameters necessary to decode transmissions particular to an individual network, enhances the efficiency of the analyzer to decode data.

If you have decoders loaded which require decoder parameters, a window with one tab for every decoder that requires parameters appears the first time the decoder is loaded.

For help on setting the parameters, click the **Help** button on each tab to get help information specific to that decoder.

If you need to change the parameters later,

- Choose **Set Initial Decoder Parameters...** from the **Options** menu on the **Control** and **Frame Display** windows.

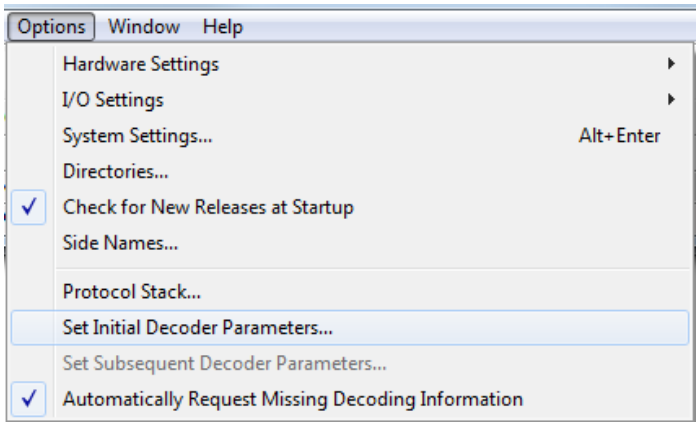


Figure 3.15 - Select **Set Initial Decoder Parameters...** from **Control** window

The **Set Initial Decoder Parameters** window opens with a tab for each decoder that requires parameters.

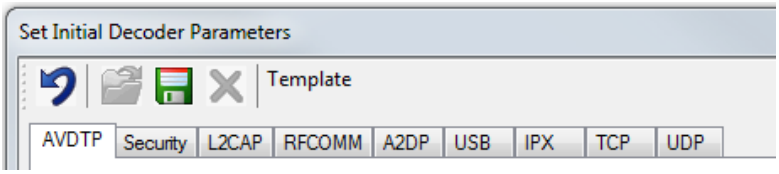


Figure 3.16 - Tabs for each decoder requiring parameters.

- Each entry in the **Set Initial Decoder Parameters** window takes effect from the beginning of the capture onward or until redefined in the **Set Subsequent Decoder Parameters** dialog.

Override Existing Parameters

The **Set Subsequent Decoder Parameters** dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter

- Select the frame where the change should take effect
  - Select **Set Subsequent Decoder Parameters...** from the **Options** menu, and make the needed changes. You can also right-click on the frame to select the same option.

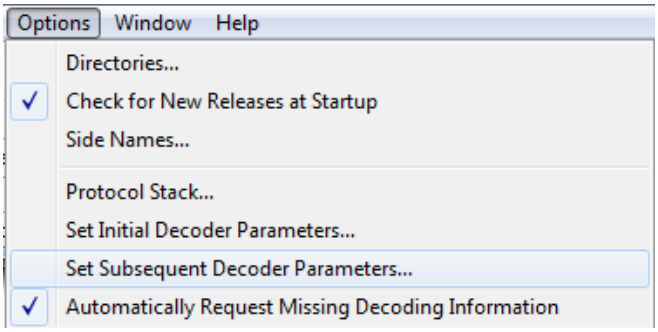


Figure 3.17 - **Set Subsequent Decoder Parameters...** from **Control** window

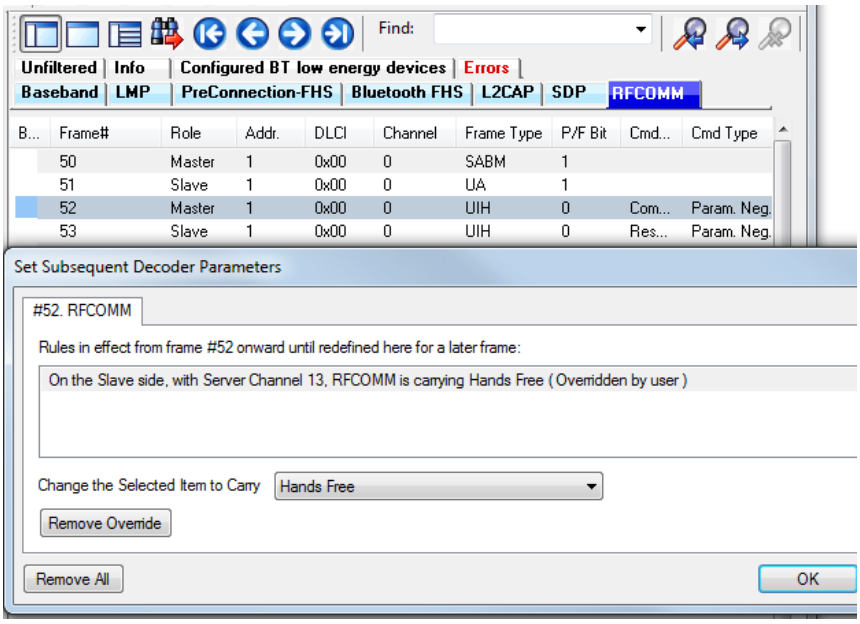


Figure 3.18 - Example: Set Subsequent Decode for Frame #52, RFCOMM

- Each entry in the **Set Subsequent Decoder Parameters** dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.
- The **Remove Override** button will remove the selected decode parameter override.
- The **Remove All** button will remove all decoder overrides.

If you do not have decoders loaded that require parameters, the menu item does not appear and you don't need to worry about this feature.

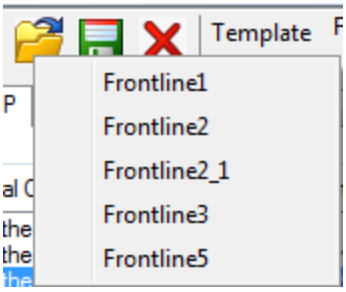
3.2.1 Decoder Parameter Templates

3.2.1.1 Select and Apply a Decoder Template

1. Select **Set Initial Decoder Parameters...** from the **Options** menu on the **Control** window or the **Frame Display**

window.

2. Click the **Open Template** icon in the toolbar and select the desired template from the pop up list. The system displays the content of the selected template in the Initial Connections list at the top of the dialog



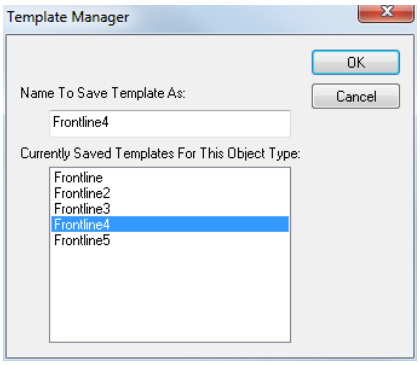
3. Click the OK button to apply the selected template and decoders' settings and exit the **Set Initial Decoder Parameters** dialog.

3.2.1.2 Adding a New or Saving an Existing Template

Add a Template

A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

1. Click the **Save** button at the top of the **Set Initial Decoder Parameters** dialog to display the **Template Manager** dialog.



2. Enter a name for the new template and click **OK**.

   The system saves the template and closes the **Template Manager** dialog.

3. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the template and close the dialog.

Save Changes to a Template

This procedure saves changes to parameters in an existing template.

1. After making changes to parameter settings in a user defined template, click the **Save** button at the top of the **Set Initial Decoder Parameters** window to display the **Template Manager** dialog.
2. Ensure that the name of the template is listed in the **Name to Save Template As** text box and click **OK**.
3. The system displays a dialog asking for confirmation of the change to the existing template. Click the **Yes** button.

   The system saves the parameter changes to the template and closes the Save As dialog.

4. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the template and close the window.

3.2.1.3 Deleting a Template

1. After opening the **Set Initial Decoder Parameters** window click the **Delete** button in the toolbar.

   The system displays the **Template Manager** dialog with a list of saved templates.

2. Select (click on and highlight) the template marked for deletion and click the **Delete** button.

   The system removes the selected template from the list of saved templates.

3. Click the **OK** button to complete the deletion process and close the Delete dialog.

4. Click the **OK** button on the **Set Initial Decoder Parameters** window to apply the deletion and close the dialog.

3.2.2 Wi-Fi Security Decoder Parameters

On the Set Initial Decoder Parameters dialog, the security tab allows specifying a key for software decryption of 802.11 frames.

To access this dialog:

1. In the **Options** menu on the **Control** window and choose **Set Initial Decoder Parameters.**

2. Select the **Security** tab.

There are three types of types of encrypted data on the security tab, each one selectable via a radio button.

- WPA2 (Wi-Fi Protected Access), and WEP (Wired Equivalent Privacy) data that is transmitted over a 802.11 communications link. There are two values you have to enter for the WPA2 and WEP to be decrypted properly. Click here to see additional WEP settings in the I/O Settings dialog.
- The Bluetooth® alternative MAC/PHY (AMP) enables *Bluetooth* to support data rates up to 24Mbps by using additional wireless radio technologies.
- The third method is to specify the pre-shared key in its raw hex forum a 32-byte hex number.

Depending on which **Encrypted Data** type you select, the options for entering data on the rest of the dialog varies.

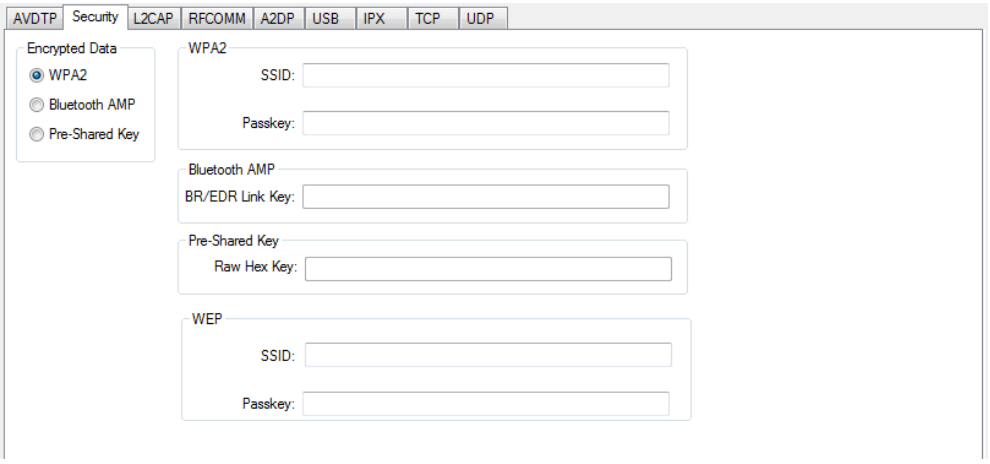


Figure 3.19 - Security (WPA2/WEP) Decoder Tab

Set the WPA2 or WEP parameters.

1. Select the **WPA2** radio button. This activates the **WPA2** and **WEP** text boxes.
2. There are two values to set for the **WPA2** and **WEP** keys.
    a. **WEP SSID** (Service Set Identifiers) - the station ID of the 802.11 communications link.
    b. **WEP Passkey** - .the shared passkey phrase used in communications.
3. Select **OK** to save the settings and close the dialog.

Set the Bluetooth AMP parameters.

Bluetooth AMP parameters are used when capturing 802.11 alternative MAC/PHY (AMP) frames for **Bluetooth** High Speed.

1. Select the **Bluetooth AMP** radio button to activate **Bluetooth AMP** and **WEP** text boxes
2. Enter a hexadecimal value for the **BR/EDR Link Key** (Basic Rate or Extended Data Rate) .
3. There are two values to set for the WEP key.
    a. **WEP SSID** (Service Set Identifiers) - the station ID of the 802.11 communications link.
    b. **WEP Passkey** - .the shared passkey phrase used in communications.

Note: When capturing both *Bluetooth* and 802.11 data using the 802.11 AMP capture selection, Frontline uses the link from the BR/EDR connection. To automatically decode 802.11 AMP frames in this case, select the *Bluetooth* AMP encryption type but leave the link key blank.

4. Select **OK** to save the settings and close the dialog.

Set the Pre-Shared Key parameters.

The third way to set encrypted data is to specify the pre-shared key in its raw hex forumas a 32-byte hex number.

Note: The other ways of specifying the WPA2 key automatically generate this value.

1. Select the **Pre-Shared Key** radio button - activates the **Pre-Shared Key** and **WEP** text boxes.
2. Enter a 32-byte hex number inthe **Pre-Shared Key Raw Hex Key** text box.
3. There are two values to set for the WEP key.
    a. **WEP SSID** (Service Set Identifiers) - the station ID of the 802.11 communications link.
    b. **WEP Passkey** - .the shared passkey phrase used in communications.

Note: When capturing both *Bluetooth* and 802.11 data using the 802.11 AMP capture selection, Frontline uses the link from the BR/EDR connection. To automatically decode 802.11 AMP frames in this case, select the *Bluetooth* AMP encryption type but leave the link key blank.

4. Select **OK** to save the settings and close the dialog.

3.2.3 Adding or Changing TCP/UDP Port Assignments

TCP and UDP are Transport layer protocols in the IP protocol suite. These transport layer protocols use ports to establish communication between application layer protocols. For example, all Web traffic uses the HTTP protocol. HTTP is an application layer protocol that uses the standard TCP/UDP port 80. The Internet Assigned Numbers Authority (IANA) is responsible for maintaining the list of standard port numbers and their assignments. For an up-to-date listing of all standard TCP/UDP port assignments, visit www.iana.org.

When the analyzer reads a TCP, UDP or IPX packet, it infers the upper layer protocols by using pre-defined rules of traversal. For example, if the packet has a TCP source or destination port number 80, then the upper layer protocol is HTTP. These rules, which are built in to the software, determine the upper layers of the protocol stack based on the source or destination port numbers in the packet. The built-in rules are based on the standard port assignments. However, it is quite common to come across network systems in which upper layer protocols use user-defined port numbers for both standard and custom protocols. In such cases, the analyzer users can tell the software which port numbers are assigned to which protocols.

The analyzer autotraverses the stack from TCP, UDP and IPX based on the source or destination port number. Many systems use user-defined port numbers for both standard and custom protocols. Here's how to tell the analyzer about a custom port assignment on the system you are monitoring.

Add a New Port Assignment

1. Choose Set Initial Decoder Parameters from the Options menu on the Control window.
2. Click the TCP tab (or UDP or IPX for those protocols).
3. Choose the Single Port radio button
4. Enter the port number in the Port Number box.
5. In the Protocol drop-down list, choose the protocol to traverse to.
6. Click the Add button.

The system adds the new entry to the bottom of the port number list.

Modify an Existing Port Assignment

1. Choose **Set Initial Decoder Parameters** from the **Options** menu on the Control window.
2. Click the **TCP** tab (or **UDP** or **IPX** for those protocols).
3. Select (click on and highlight) the port assignment to modify.
4. Change the port number and/or choose the protocol to traverse to.
5. Select the **Port Range** radio button and specify the starting and ending port numbers. The range is inclusive.
6. Click the **Modify** button.

The system displays the changes in port assignment.

Delete a Port Assignment

1. Choose **Set Initial Decoder Parameters** from the **Options** menu on the Control window.
2. Click the **TCP** tab (or **UDP** or **IPX** for those protocols).
3. Select (click on and highlight) the port assignment to delete.
4. Select **Delete**.

The system deletes the port assignment.

Move a Port Assignment

If you need to move an entry to ensure it is processed before or after another entry, select the entry in the list and then click the **Move Up** or **Move Down** buttons.

Port Assignment Considerations

- The analyzer traverses an entry if either the source or destination port match.
- The analyzer processes port number entries in order from top to bottom.

Chapter 4 Capturing and Analyzing Data

The following sections describe the various ComProbe software functions that capture and display data packets.

4.1 Capture Data

4.1.1 Air Sniffing: Positioning Devices

When capturing over the air packets, proper positioning of the ComProbe hardware and the Devices Under Test (DUTs) will result in the best possible captures and will mitigate sources of path loss and interference. The following procedures will help optimize the capture process especially if you are have problems obtaining reliable …captures.

Problems with indoor radio propagation

Even in free space, it is well understood that radio frequencies attenuate over distance. The free-space rule-of-thumb dictates that radio energy decreases in strength by 20 dB by each 10-to-1 increase in range. In the real-world, the effects of objects in an outdoor environment cause reflection, diffraction, and scattering resulting in greater signal losses. Indoors the situation can be worse. Reflections occur from walls and other large flat surfaces. Diffraction occurs from objects with sharp edges. Scattering is produced from objects with rough surfaces and from small objects. Also any object directly in the path of the radiation can present a hard or soft partition depending on the partition's material properties. Path losses from partitions are difficult to estimate.

Estimating indoor propagation loss

One estimate of indoor path loss, based on path loss data from a typical building, provides a $\frac{1}{range^{3.5}}$ power rule. At 2.4 GHz, the following relationship provides an approximate estimate of indoor path loss:

$$Indoor\ Path\ Loss\ (in\ dB) = 40 + 35Log_{10}(range,\ in\ meters)$$

This approximation is expected to have a variance of 13 dB.

Mitigating path loss and interference

Bluetooth device design contributes to mitigating environmental effects on propagation through spread spectrum radio design, for example. However, careful planning of the testing environment can also contribute to reliable data capture process.

The first step to ensuring reliable air-sniffing data capture is to understand the RF characteristics of the Devices Under Test (DUTs). The *Bluetooth* Class, antenna types, and radiation patterns are all important factors that can affect the placement of the DUTs and the ComProbe analyzer. Radiation patterns are rarely spherical, so understanding your device's radiation patterns can greatly enhance successful data capture. Position devices to avoid radiation attenuation by the surroundings.

This step is optional: Consider conductive testing to establish a baseline capture. Conductive testing isolates the DUTs and analyzer from environmental effects.

The next step is to ensure that the testing environment is as clutter-free as possible.

- Line-of-sight obstructions should be eliminated between the ComProbe hardware and the DUTs because they cause a reduction in signal strength. Obstructions include, but are not limited to: water bottles, coffee cups, computers, computer screens, computer speakers, and books. A clear, unobstructed line-of-sight is preferred for DUT and ComProbe hardware positioning.
- If using an analyzer connected to a computer, position the computer on an adjacent table or surface away from the analyzer and DUTs, taking advantage of the cables' length. If this is not possible, position the computer behind the analyzer as far away as possible. If using the ComProbe FTS4BT, which is a dongle, either use an extension USB cable or position the computer such that the dongle is positioned towards the DUTs.
- The preferred placement is positioning the DUTs and the ComProbe hardware at the points of an equilateral triangle in the same horizontal plane, i.e. placed on the same table or work surface. The sides of the triangle should be between 1 and 2 meters for Bluetooth transmitter classes 1 and 2. The distance for transmitter class 3 should be 1/2 meter.

Figure 4.1 - Devices Equally Spaced in the Same Horizontal Plane

Finally, eliminate other RF sources.

- Wi-Fi interference should be minimized or eliminated. *Bluetooth* shares the same 2.4 GHz frequency bands as Wi-Fi technology. Wi-Fi interference can cause loss of packets and poor captures. In a laboratory or testing

environment do not place the DUTs and ComProbe hardware in close proximity with Wi-Fi transmitting sources such as laptops or routers. Turning off Wi-Fi on the computer running the ComProbe software is recommended.

Poor Placement

A poor test configuration for the analyzer is placing the DUTs very close to each other and the analyzer far away. The DUTs, being in close proximity to each other, reduce their transmission power and thus make it hard for the analyzer to hear the conversation. If the analyzer is far away from DUTs, there are chances that the analyzer may miss those frames, which could lead to failure in decryption of the data.

Obstacles in close proximity to or in between the analyzer and the DUTs can interfere and cause reduction in signal strength or interference. Even small objects can cause signal scattering.

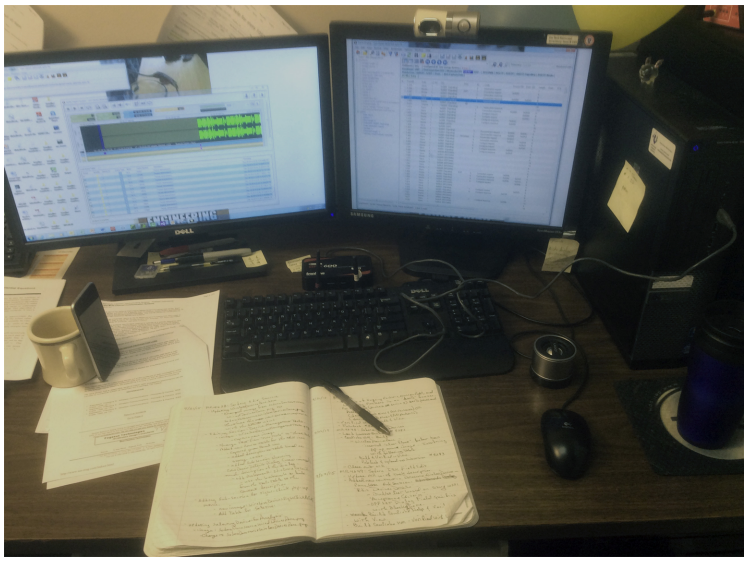


Figure 4.2 - Example: Poor Capture Environment

4.1.2 Capturing Data to Disk - General Procedure

Note: Capture is not available in Viewer mode.

1. Click the **Start Capture** button to begin capturing to a file. This icon is located on the **Control** , **Event Display**, and **Frame Display** windows.
2. Files are placed in My Capture Files by default and have a .cfa extension. Choose **Directories** from the **Options** menu on the **Control** window to change the default file location.

   Note: For the Dashboard, when you capture to series of files, the window displays the data from the beginning of the first capture, even when a new file in the series is created. This is because the Dashboard is a "Session Monitor", which means that even if you capture to a series of files, the data from the first file is always displayed. The display does not refresh when a new capture file in a series is created.
3. Watch the status bar on the **Control** window to monitor how full the file is. When the file is full, it begins to **wrap**, which means the oldest data will be overwritten by new data.

4. Click the **Stop Capture** icon to temporarily stop data capture. Click the **Start Capture** icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured data remains in the file.
5. To clear captured data, click the **Clear** icon .

- If you select **Clear** after selecting **Stop Capture**, a dialog appears asking whether you want to save the data.
  - You can click **Save File** and enter a file name when prompted .
  - If you choose **Do Not Save**, all data will be cleared.
  - If you choose **Cancel,** the dialog closes with no changes.
- If you select the **Clear** icon while a capture is occurring:
  - The capture stops.
  - A dialog appears asking if you want to save the capture
  - You can select **Yes** and save the capture or select **No** and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
  - If you choose **Cancel**, the dialog closes with no changes.

To see how to capture to a single file, choose System Settings from the Options menu on the Control window.

When live capture stops, no new packets are sniffed but there can still be packets that were previously sniffed but not yet read by the ComProbe analyzer. This happens when packets are being sniffed faster than the ComProbe analyzer can process them. These packets are stored either on the ComProbe hardware itself or in a file on the PC. If there are remaining packets to be processed when live capture stops the **Transferring Packets** dialog below is displayed showing the packets yet to be read by the ComProbe analyzer. The dialog shows the name of each ComProbe hardware device, its process id in square brackets, and the number of packets remaining. These stored packets are read until they're exhausted or the user clicks the Discard button on the dialog.

Unlike 802.11, *Bluetooth* packets never come in faster than the datasource can process them. However, *Bluetooth* packets must still be stored so that they can be read in chronological order with the 802.11 packets.

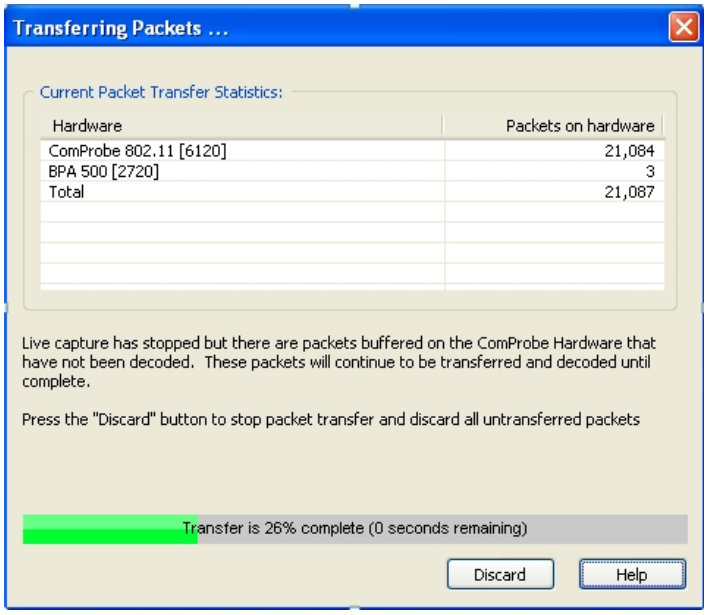

Transferring Packets ...
Current Packet Transfer Statistics:
Hardware
Packets on hardware
ComProbe 802.11 [6120]
21,084
BPA 500 [2720]
3
Total
21,087
Live capture has stopped but there are packets buffered on the ComProbe Hardware that have not been decoded. These packets will continue to be transferred and decoded until complete.
Press the "Discard" button to stop packet transfer and discard all untransferred packets
Transfer is 26% complete (0 seconds remaining)
Discard
Help

Figure 4.3 - Packet Transfer Dialog

4.1.2.1 ComProbe 802.11 with Wireshark®

4.1.3 Capturing Using Frontline Wi-Fi Datasource with Wireshark®

Note: This topic is provided as a courtesy to our customers who want to use Wireshark in conjunction with the ComProbe 802.11 although the ComProbe software is fully capable of performing the same functions as Wireshark. Frontline does not support or maintain third party products. Should you have difficulty with your Wireshark product contact the manufacturer for support or maintenance.

Click on the "ComProbe 802.11 with Wireshark" short cut to launch and start capturing the Wi-Fi packets. If you do not see any packets on the Wireshark window then check the status message indication on the **Wi-Fi Datasource** window to see if sniffing has stopped. Click on the **Start** button .

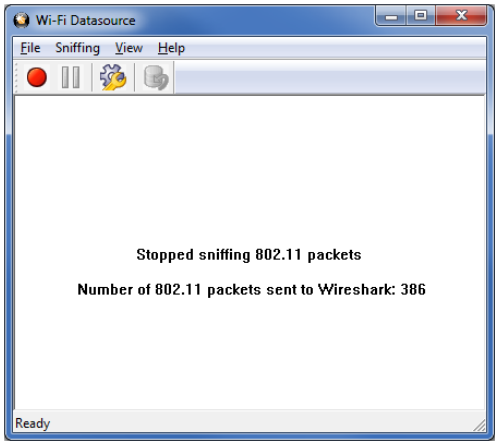


Figure 4.4 - Datasource Stopped Sniffing

When the ComProbe 802.11 is sniffing the datasource will display the following message. Sniffing can be stopped by clicking the **Stop** button .

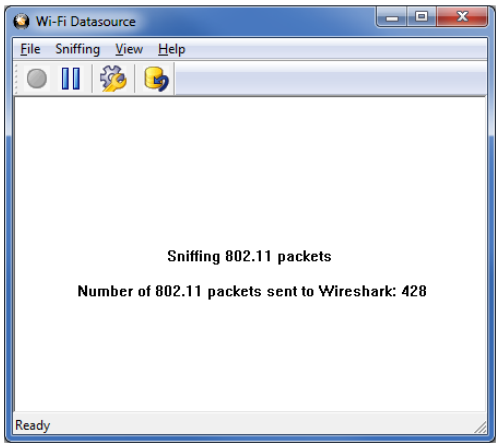


Figure 4.5 - Datasource Sniffing

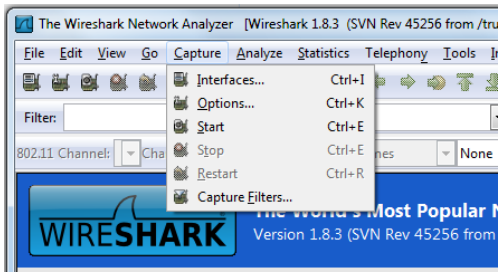


Figure 4.6 - Wireshark Capture Dialog

Note: Whenever you give Start Capture command on Wireshark, the status message on the Wi-Fi Datasource window should display "Please START capturing on the Wireshark." If it is displaying a different message then you can use the Reset button on the Wi-Fi Datasource window or select **Reset** or in the Sniffing menu to get back to this message.

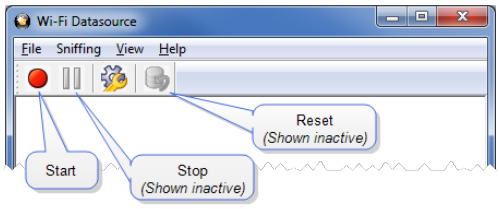


Figure 4.7 - Wi-Fi Datasource Toolbar

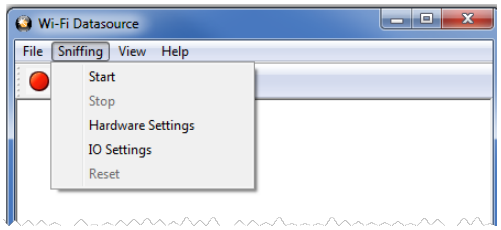


Figure 4.8 - Wi-Fi Datasource Sniffing Menu

Once the Wi-Fi Datasource starts capturing packets and sending them to Wireshark, you can pause and resume capturing using the **Stop** and **Start** toolbar buttons on the Wi-Fi Datasource toolbar or the **Sniffing** menu. Note that the **Restart** command on the Wireshark window does not function. The workaround is to click **Reset** on the Wi-Fi Datasource then click **Start** on the Wireshark Capture menu. Also the Wireshark Capture Filters menu does not function, but you can use IO Settings menu on the Wi-Fi Datasource window or **Sniffing** menu for setting filters.

Known Issues with Wireshark

- In Real Time capture mode (when you select Update list of packets in real time check-box in the Capture Options dialog), if you move the Wireshark window around on the desktop or click on anything on the Wireshark window, it freezes the desktop. You can unfreeze it by bringing up Windows Task Manager by pressing Ctrl+Alt+Delete.

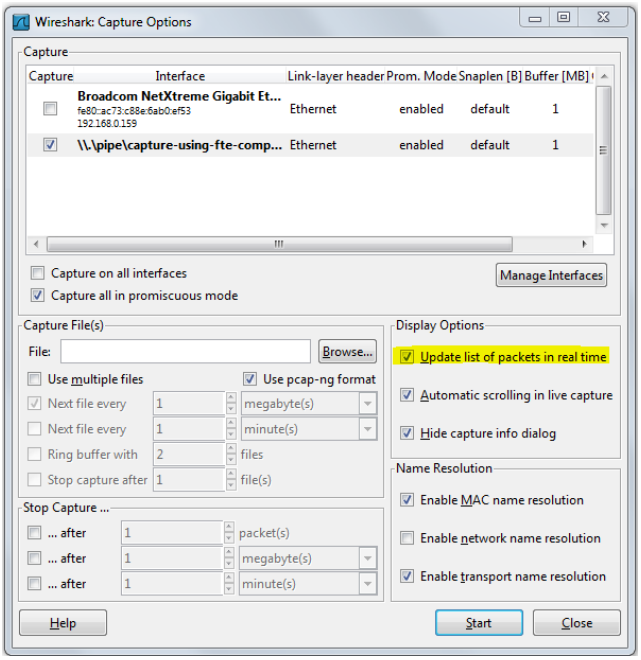


Figure 4.9 - Wireshark Capture Options

- If you capture more than a few millions of packets, e.g. 4 million, Wireshark crashes.

4.1.4 Combining BPA 600, 802.11, and HSU with ProbeSync

ProbeSync™ allows multiple ComProbe analyzers to work seamlessly together and to share a common clock. Clock sharing allows the analyzers to precisely synchronize communications stream and to display resulting packets in a single shared view.

The ComProbe BPA 600, ComProbe 802.11, and ComProbe HSU analyzers have ProbeSync capability allowing timestamp synchronization of captured data. Synchronizing the clock for these ComProbe devices used in combination requires attention to the sequence of hardware connection. It is important to remember the following key points.

- ComProbe devices are connected serially in a daisy-chain fashion. The combined length of all cables in the chain cannot exceed 1.5 meters (4.5 ft.).
- The "master" ComProbe device provides the clock to the other devices. All other ComProbe devices are "slaves" and received the clock from the "master" device.
- On ComProbe devices with an **OUT** and **IN** connector, the function of these connectors is dependent on if they are a "master" or a "slave".
    - "master" device: **OUT** connector provides the clock to all "slave" devices. **IN** connector is not used.
    - "slave" device: **IN** connector receives the clock from the **OUT** connector of the prior device in the chain. The **OUT** connector is just a pass-through connector on a "slave" device.
- BPA 600 is always the "master" device and the first device in the chain, if being used.
- HSU is always the last "slave" device in the chain, if being used.
- HSU maximum capture data rate is 6 Mbit/sec.

Connecting ComProbe BPA 600, ComProbe 802.11, and ComProbe HSU devices in ProbeSync takes place in the following steps.

1. Connect the ComProbe BPA 600 **OUT** connector to the ComProbe 802.11 **IN** connector.
2. Connect the ComProbe HSU Cat 5 cable to the ComProbe 802.11 **OUT** connector.

Each device datasource is setup individually to sniff their respective link. Should the hardware be connected incorrectly, that is **IN** to **IN** or **OUT** to **OUT**, an error message will appear. Follow the instructions in error message. To continue click on the **OK** button. The ComProbe device datasource **Status** window will also display a warning message suggesting information sources.

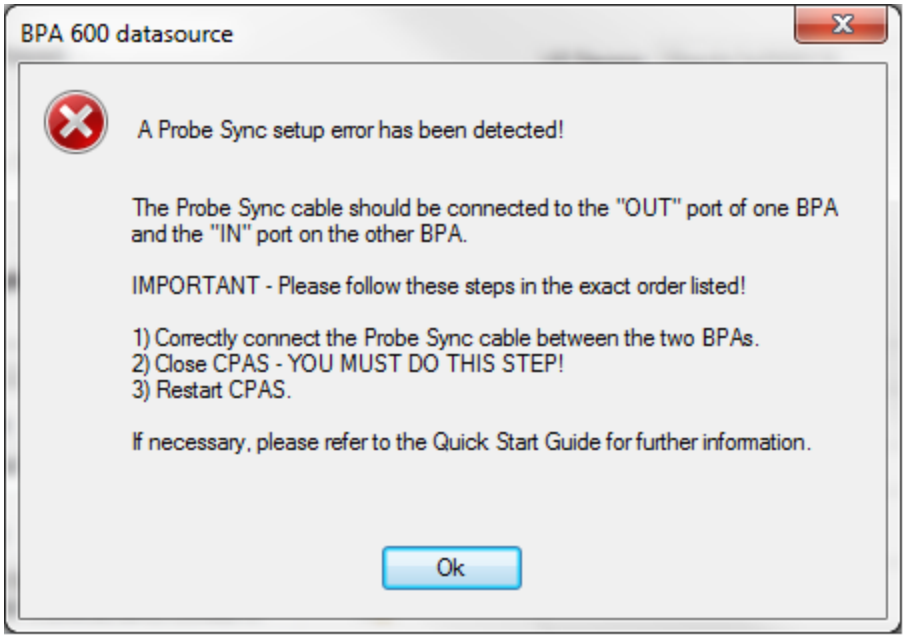

BPA 600 datasource
A Probe Sync setup error has been detected!
The Probe Sync cable should be connected to the "OUT" port of one BPA and the "IN" port on the other BPA.
IMPORTANT - Please follow these steps in the exact order listed!
1) Correctly connect the Probe Sync cable between the two BPAs.
2) Close CPAS - YOU MUST DO THIS STEP!
3) Restart CPAS.
If necessary, please refer to the Quick Start Guide for further information.
Ok

Figure 4.10 - Incorrect ProbeSync Hardware Connection Error

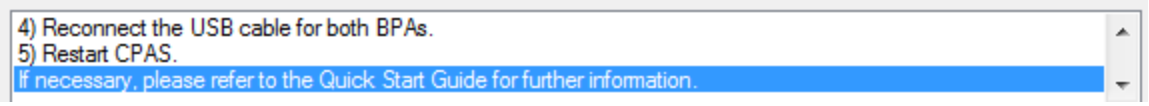

4) Reconnect the USB cable for both BPAs.
5) Restart CPAS.
If necessary, please refer to the Quick Start Guide for further information.

Figure 4.11 - Incorrect ProbeSync Hardware Connection Message In Datasource Status

The **BPA 600 datasource** dialog **Start Sniffing** button initiates the capture for all connected ComProbe 802.11 and HSU devices. On the 802.11 and HSU receiving the clock—cable connected to **IN**— the **Start Sniffing** button is disabled when using ProbeSync. In each ComProbe device's **Control** window status window will announce the synchronizing function.

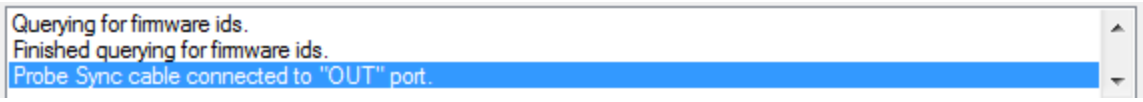


Figure 4.12 - ProbeSync Synchronizing Device Status Message

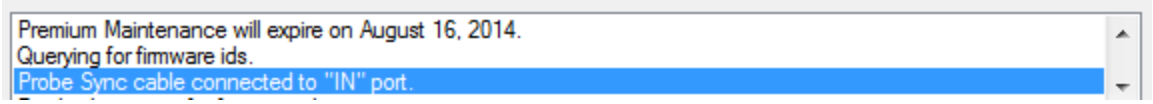


Figure 4.13 - ProbeSync Synchronized Device Status Message

Data captured in the synchronized device will appear in the **Frame Display**, **Event Display**, **Bluetooth Timeline**, **Bluetooth low energy Timeline**, and **Coexistence View**. Data saved as a capture file will include data captured on each devices. Within these dialogs the packets identified as link 1, 2, and 3 were captured on the synchronizing device that provides the clock. Those packets captured on the synchronized device carry link 4, 5, and 6 identifiers.

4.1.5 Extended Inquiry Response

Extended Inquiry Response (EIR) is a tab that appears automatically on the **Frame Display** window when you capture data.

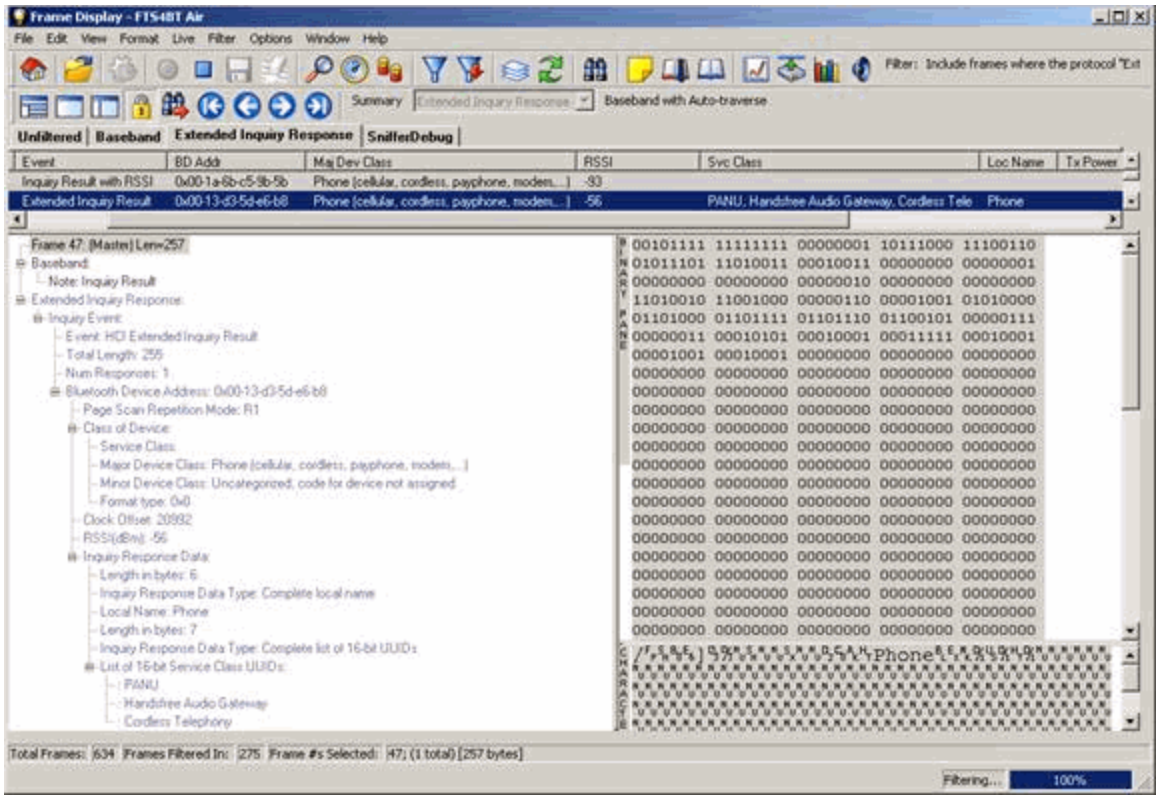


Figure 4.14 - Frame Display Extended Inquire Response

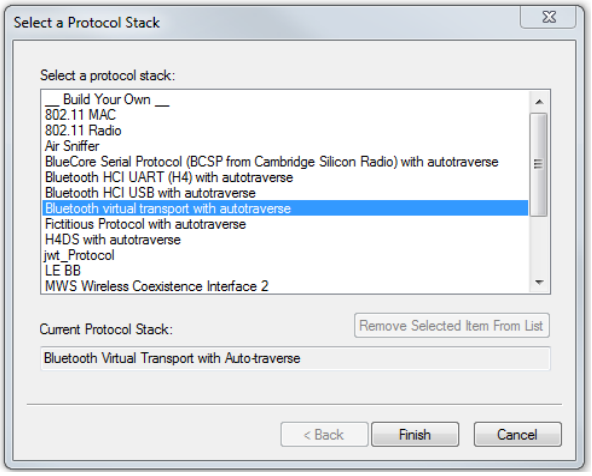
EIR displays extensive information about the Bluetooth® devices that are discovered as data is being captured. EIR provides more information during the inquiry procedure to allow better filtering of devices before connection; and sniff subrating, which reduces the power consumption in low-power mode. Before the EIR tab was created, this type of information was not available until a connection was made to a device. Therefore, EIR can be used to determine whether a connection can/should be made to a device prior to making the connection.

Note: If a *Bluetooth* device does not support **Extended Inquiry Response**, the tab displays **Received Signal Strength Indication** (RSSI) data, which is less extensive than EIR data.

4.2 Protocol Stacks

4.2.1 Protocol Stack Wizard

The Protocol Stack wizard is where you define the protocol stack you want the analyzer to use when decoding frames.



To start the wizard:

1. Choose **Protocol Stack** from the **Options** menu on the **Control** window or click the **Protocol Stack** icon on the **Frame Display**.
2. Select a protocol stack from the list, and click **Finish**.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, see Creating and Removing a Custom Stack on page 48.

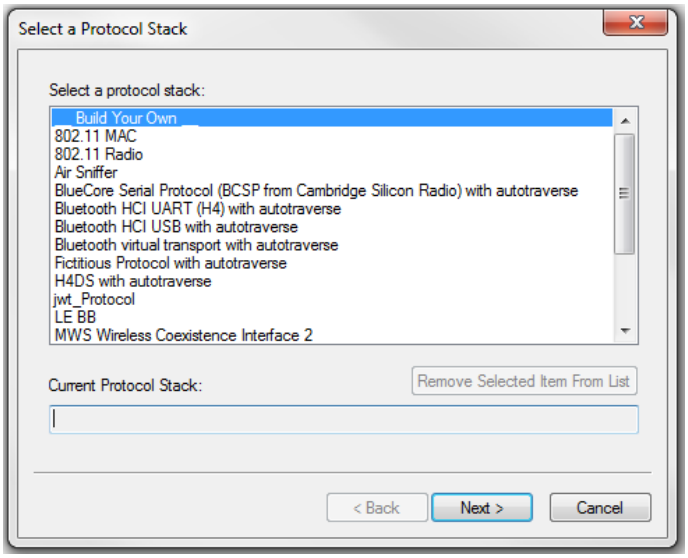
1. If you select a custom stack (i.e. one that was defined by a user and not included with the analyzer), the **Remove Selected Item From List** button becomes active.
2. Click the **Remove Selected Item From List**button to remove the stack from the list. You cannot remove stacks provided with the analyzer. If you remove a custom stack, you need to define it again in order to get it back.

If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing on page 49 for more information.

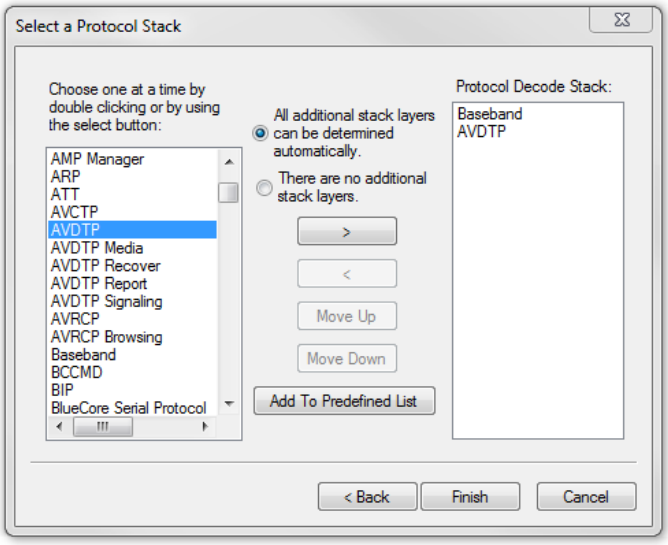
You cannot select a stack or change an existing one for a capture file loaded into the Capture File Viewer (the Capture File Viewer is used only for viewing capture files and cannot capture data). Protocol Stack changes can only be made from a live session.

4.2.2 Creating and Removing a Custom Stack

To create a custom stack:



1. Choose **Protocol Stack** from the **Options** menu on the **Control** window or click the Protocol Stack icon on the **Frame Display** toolbar.
2. Select **Build Your Own** from the list and click **Next**.
3. The system displays an information screen that may help you decide if you need to define your own custom stack. Defining a custom stack means that the analyzer uses the stack for every frame. Frames that do not conform to the stack are decoded incorrectly. Click **Next** to continue.



Select Protocols

1. Select a protocol from the list on the left.
2. Click the right arrow button to move it to the **Protocol Decode Stack** box on the right, or double-click the protocol to move it to the right.
3. To remove a protocol from the stack, double-click it or select it and click the left arrow button.
4. If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the **Move Up** and **Move Down** buttons until the protocol is in the correct position.
5. The lowest layer protocol is at the top of the list, with higher layer protocols listed underneath.

Auto-traversal (Have the analyzer Determine Higher Layers)

If you need to define just a few layers of the protocol stack, and the remaining layers can be determined based on the lower layers:

1. Click the **All additional stack layers can be determined automatically** button.
2. If your protocol stack is complete and there are no additional layers, click the **There are no additional stack layers** button.

3. If you select this option, the analyzer uses the stack you defined for every frame. Frames that do use this stack are decoded incorrectly.

Save the Stack

1. Click the Add To Predefined List button.
2. Give the stack a name, and click Add.

In the future, the stack appears in the **Protocol Stack List** on the first screen of the Protocol Stack wizard.

Remove a Stack

1. Select it in the first screen and click Remove Selected Item From List.
2. If you remove the stack, you must to recreate it if you need to use it again.

Note: If you do not save your custom stack, it does appear in the predefined list, but applies to the frames in the current session. However, it is discarded at the end of the session.

4.2.3 Reframing

If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you need to reframe in order for the protocol decode to be correct. You can also use **Reframe** to frame unframed data. The original capture file is not altered during this process.

Note: You cannot reframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To reframe your data, load your capture file, select a protocol stack, and then select **Reframe** from the **File** menu on the **Control** window. **Reframe** is only available if the frame recognizer used to capture the data is different from the current frame recognizer.

In addition to choosing to **Reframe**, you can also be prompted to Reframe by the Protocol Stack Wizard.

1. Load your capture file by choosing **Open** from the **File** menu on the **Control** window, and select the file to load.
2. Select the protocol stack by choosing **Protocol Stack** from the **Options** menu on the **Control** window, select the desired stack and click **Finish**.
3. If you selected a protocol stack that includes a frame recognizer different from the one used to capture your data, the **Protocol Stack Wizard** asks you if you want to reframe your data. Choose **Yes**.
4. The analyzer adds frame markers to your data, puts the framed data into a new file, and opens the new file. The original capture file is not altered.

See Unframing on page 49 for instructions on removing framing from data.

4.2.4 Unframing

This function removes start-of-frame and end-of-frame markers from your data. The original capture file is not altered during this process. You cannot unframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To manually unframe your data:

1. Select **Unframe** from the **File** menu on the **Control** window. **Unframe** is only available if a protocol stack was used to capture the data and there is currently no protocol stack selected.

In addition to choosing to **Unframe**, you can also be prompted to Unframe by the Protocol Stack Wizard.

1. Load your capture file by choosing **Open** from the **File** menu on the **Control** window.
2. Select the file to load.
3. Choose **Protocol Stack** from the **Options** menu on the **Control** window
4. Select **None** from the list
5. Click **Finish**. The Protocol Stack Wizard asks you if you want to unframe your data and put it into a new file.
6. Choose **Yes**.

The system removes the frame markers from your data, puts the unframed data into a new file, and opens the new file. The original capture file is not altered.

See Reframing on page 49 for instructions on framing unframed data.

4.2.5 How the Analyzer Auto-traverses the Protocol Stack

In the course of doing service discovery, devices ask for and receive a Protocol Descriptor List defining which protocol stacks the device supports. It also includes information on which PSM to use in L2CAP, or the channel number for RFCOMM, or the port number for TCP or UDP. The description below talks about how the analyzer auto-traverses from L2CAP using a dynamically assigned PSM, but the principle is the same for RFCOMM channel numbers and TCP/UDP port numbers.

The analyzer looks for SDP Service Attribute Responses or Service Search Attribute Responses carrying protocol descriptor lists. If the analyzer sees L2CAP listed with a PSM, it stores the PSM and the UUID for the next protocol in the list.

After the SDP session is over, the analyzer looks at the PSM in the L2CAP Connect frames that follow. If the PSM matches one the analyzer has stored, the analyzer stores the source channel ID and destination channel ID, and associates those channel IDs with the PSM and UUID for the next protocol. Thereafter, when the analyzer sees L2CAP frames using those channel IDs, it can look them up in its table and know what the next protocol is.

In order for the analyzer to be able to auto-traverse using a dynamically assigned PSM, it has to have seen the SDP session giving the Protocol Descriptor Lists, and the subsequent L2CAP connection using the PSM and identifying the source and channel IDs. If the analyzer misses any of this process, it is not able to auto-traverse. It stops decoding at the L2CAP layer.

For L2CAP frames carrying a known PSM (0x0001 for SDP, for example, or 0x0003 for RFCOMM), the analyzer looks for Connect frames and stores the PSM along with the associated source and destination channel IDs. In this case the analyzer does not need to see the SDP process, but does need to see the L2CAP connection process, giving the source and destination channel IDs.

4.2.6 Providing Context For Decoding When Frame Information Is Missing

There may be times when you need to provide information to the analyzer because the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame

indicating the command.

The analyzer provides a way for you to supply the context for any frame, provided the decoder supports it. (The decoder writer has to include support for this feature in the decoder, so not all decoders support it. Note that not all decoders require this feature.)

If the decoder supports user-provided context, three items are active on the **Options** menu of the **Control** window and the **Frame Display** window. These items are **Set Initial Decoder Parameters**, **Automatically Request Missing Decoding Information**, and **Set Subsequent Decoder Parameters**. (These items are not present if no decoder is loaded that supports this feature.)

Set Initial Decoder Parameters is used to provide required information to decoders that is not context dependent but instead tends to be system options for the protocol.

Choose **Set Initial Decoder Parameters** in order to provide initial context to the analyzer for a decoder. A dialog appears that shows the data for which you can provide information.

If you need to change this information for a particular frame :

1. Right-click on the frame in the Frame Display window
2. Choose Provide <context name>.

Alternatively, you can choose **Set Subsequent Decoder Parameter** from the **Options** menu.

3. This option brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check **Automatically Request Missing Decoding Information.**
5. When unchecked, the analyzer doesn't bother you with dialogs asking for frame information that you don't have. In this situation, the analyzer decodes each frame until it cannot go further and then simply stop decoding.

4.3 Analyzing Byte Level Data

4.3.1 Event Display

To open this window click the **Event Display** icon on the **Control** window toolbar.

The **Event Display** window provides detailed information about every captured event. Events include data bytes, data related information such as start-of-frame and end-of-frame flags, and the analyzer information, such as when the data capture was paused. Data bytes are displayed in hex on the left side of the window, with the corresponding ASCII character on the right.

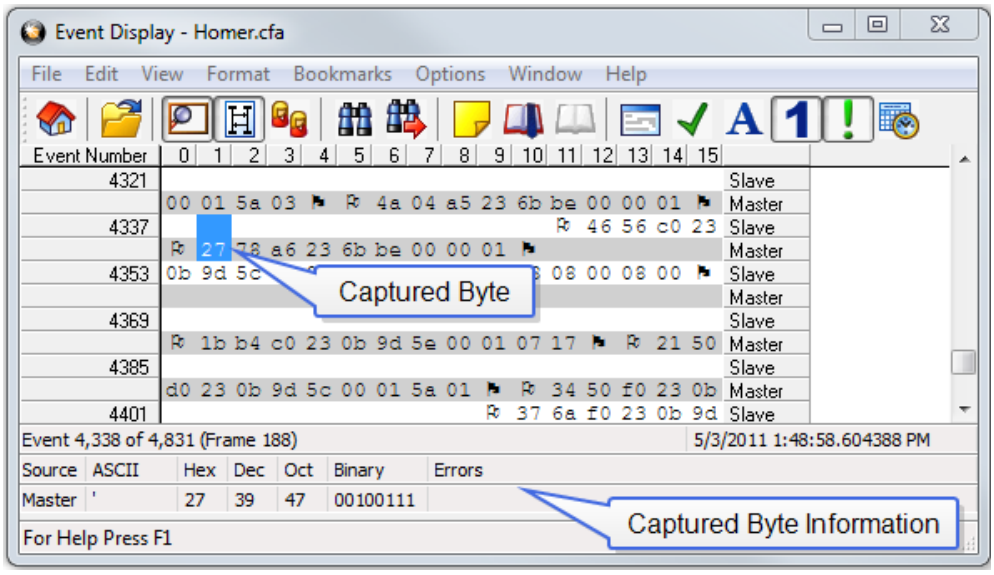

Event Display - Homer.cfa
File Edit View Format Bookmarks Options Window Help
Event Number
Captured Byte
Event 4,338 of 4,831 (Frame 188)
5/3/2011 1:48:58.604388 PM
Source ASCII Hex Dec Oct Binary Errors
Master ' 27 39 47 00100111
Captured Byte Information
For Help Press F1

Figure 4.1 Event Display

Click on an event to find out more about it. The three status lines at the bottom of the window are updated with information such as the time the event occurred (for data bytes, the time the byte was captured), the value of the byte in hex, decimal, octal, and binary, any errors associated with the byte, and more.

Events with errors are shown in red to make them easy to spot.

When capturing data live, the analyzer continually updates the Event Display as data is captured. Make sure the **Lock** icon is displayed on the toolbar to prevent the display from updating (Clicking on the icon again will unlock the display). While locked, you can review your data, run searches, determine delta time intervals between bytes, and check CRCs. To resume updating the display, click the **Lock** icon again.

You can have more than one **Event Display** open at a time. Click the **Duplicate View** icon to create a second, independent **Event Display** window. You can lock one copy of the **Event Display** and analyze your data, while the second **Event Display** updates as new data is captured.

Event Display is synchronized with the **Frame Display** and **Mesage Sequence Chart** dialogs. Selecting a byte in **Event Display** will also select the related frame in the **Frame Display** and the related message in the **Message Sequence Chart**.

4.3.2 The Event Display Toolbar

Home – Brings the Control window to the front.

Home – Brings the Control window to the front.

Start Capture - Begins data capture to disk.

Stop Capture - Closes a capture file and stops data capture to disk.

Save - Prompts user for a file name. If the user supplies a name, a .cfa file is saved.

Clear- Discards the temporary file and clears the display.

Lock - In the Lock state, the window is locked so you can review a portion of data. Data capture continues in the background. Clicking on the Lock icon unlocks the window.

Unlock - In the Unlock state, the screen fills in the data captured since the screen lock and moves down to display incoming data again. Clicking on the Unlock icon locks the window.

Duplicate View - Creates a second Event Display window identical to the first.

Frame Display - (framed data only) Brings up a Frame Display, with the frame of the currently selected bytes highlighted.

Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.

Add/Modify Bookmark - Add a new or modify an existing bookmark.

Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.

Find - Search for errors, string patterns, special events and more.

Go To - Opens the Go To dialog, where you can specify which event number to go to.

CRC - Change the algorithm and seed value used to calculate CRCs. To calculate a CRC, select a byte range, and the CRC appears in the status lines at the bottom of the Event Display.

Mixed Sides - (Serial data only) By default, the analyzer shows data with the DTE side above the DCE side. This is called DTE over DCE format. DTE data has a white background and DCE data has a gray background. The analyzer can also display data in mixed side format. In this format, the analyzer does not separate DTE data from DCE data but shows all data on the same line as it comes in. DTE data is still shown with a white background and DCE data with a gray background so that you can distinguish between the two. The benefit of using this format is that more data fits onto one screen.

Character Only - The analyzer shows both the number (hex, binary, etc.) data and the character (ASCII, EBCDIC or BAUDOT) data on the same screen. If you do not wish to see the hex characters, click on the Character Only button. Click again to go back to both number and character mode.

Number Only - Controls whether the analyzer displays data in both character and number format, or just number format. Click once to show only numeric values, and again to show both character and numeric values.

All Events - Controls whether the analyzer shows all events in the window, or only data bytes. Events include control signal changes and framing information.

Timestamping Options – Brings up the timestamping options window which has options for customizing the display and capture of timestamps.

4.3.3 Opening Multiple Event Display Windows

Click the **Duplicate View** icon from the **Event Display** toolbar to open a second **Event Display** window.

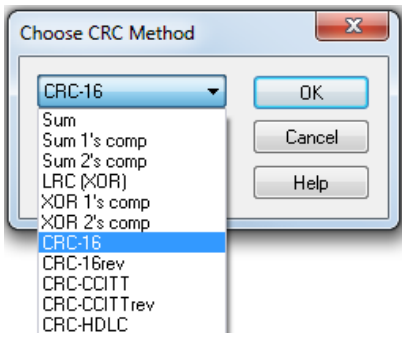
You can open as many **Event Display** windows as you like. Each **Event Display** is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

The **Event Display** windows are numbered in the title bar. If you have multiple **Event Displays** open, click on the **Event Display** icon on the **Control** window toolbar to show a list of all the **Event Displays** currently open. Select a window from the list to bring it to the front.

4.3.4 Calculating CRCs or FCSs

The cyclic redundancy check (CRC) is a function on the **Event Display** window used to produce a checksum. The frame check sequence (FCS) are the extra checksum characters added to a frame to detect errors.

1. Open the **Event Display** window.
2. Click and drag to select the data for which you want to generate a CRC.
3. Click on the **CRC** icon .
4. In the **CRC** dialog box, click on the down arrow to show the list of choices for CRC algorithms. Choose an algorithm to use. Choose CRC 32 (Ethernet). Choose CRC 32 (Ethernet) for Ethernet data or the appropriate CRC type for serial data.
5. Enter a **Seed** value in hexadecimal if desired.
6. Click **OK** to generate the CRC. It appears in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC using the algorithm you selected is calculated automatically.



Calculating CRC for interwoven data

Frontline calculates the CRC for either side of the interwoven data. Which side it calculates is determined by the first byte selected. If the first byte is from one side, then Frontline calculates the CRC for just the bytes on that side. If the first byte is from the other side, then Frontline calculates the CRC for just the bytes on that side.

Incorrect results with CRC16 for serial data

If you are calculating CRCs using the CRC16 algorithm and the CRCs do not match what you know they should be, try CRC16rev. What hardware often calls CRC16 is what software calls CRC16rev.

4.3.5 Calculating Delta Times and Data Rates

1. Click on the E**vent Display** icon on the **Control** window to open the **Event Display** window.
2. Use the mouse to select the data you want to calculate a delta time and rate for.
3. The **Event Display** window displays the delta time and the data rate in the status lines at the bottom of the window.

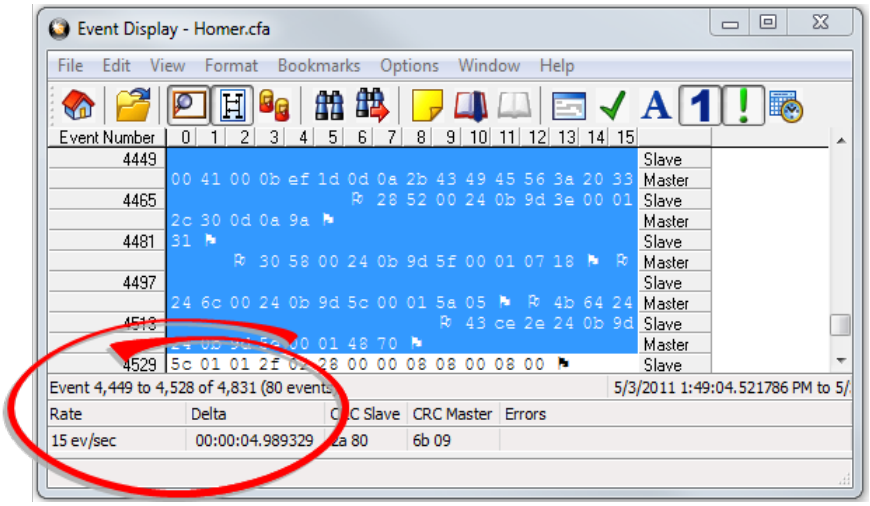


Figure 4.2 Delta fields

4.3.6 Switching Between Live Update and Review Mode

The **Event Display** and **Frame Display** windows can update to display new data during live capture, or be frozen to allow data analysis. By default, the **Event Display** continually updates with new data, and the **Frame Display** is locked.

1. Make sure the **Lock** icon is active so the display is locked and unable to scroll.
2. Click the **Unlock** icon again to resume live update.

The analyzer continues to capture data in the background while the display is locked. Upon resuming live update, the display updates with the latest data.

You can have more than one **Event Display** or **Frame Display** window open at a time. Click the **Duplicate View** icon to open additional Event or Frame Display windows. The lock/resume function is independent on each window. This means that you can have two **Event Display** windows open simultaneously, and one window can be locked while the other continues to update.

4.3.7 Data Formats and Symbols

4.3.7.1 Switching Between Viewing All Events and Viewing Data Events

By default, the analyzer on the Event Display dialog shows all **events**[1] that include:

- Data bytes
- Start-of-frame
- End-of-frame characters
- Data Captured Was Paused.

Click on the **Display All Events** icon to remove the non-data events. Click again to display all events.

See List of all Event Symbols on page 58 for a list of all the special events shown in the analyzer and what they mean.

4.3.7.2 Switching Between Hex, Decimal, Octal or Binary

On the Event Display window the analyzer displays data in Hex by default. There are several ways to change the **radix**[2] used to display data.

Go to the **Format** menu and select the radix you want. A check mark next to the radix indicates which set is currently being used.

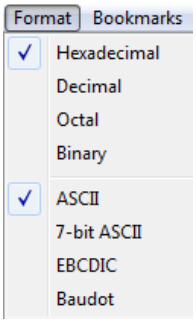


Figure 4.15 - Format Menu

[1] An event is anything that happens on the circuit or which affects data capture. Data bytes, control signal changes, and long and short breaks are all events, as are I/O Settings changes and Data Capture Paused and Resumed.
[2] The base of a number system. Binary is base 2, octal is base 8, decimal is base 10 and hexadecimal is base 16.

1. Right-click on the data display header labels and choose a different radix.

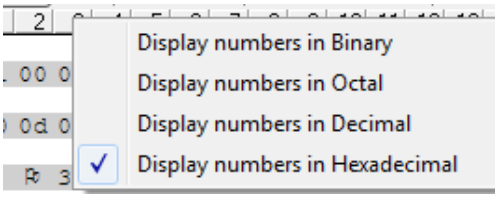


Figure 4.16 - Header labels, right click

2. Or right-click anywhere in the data display and select a different radix.

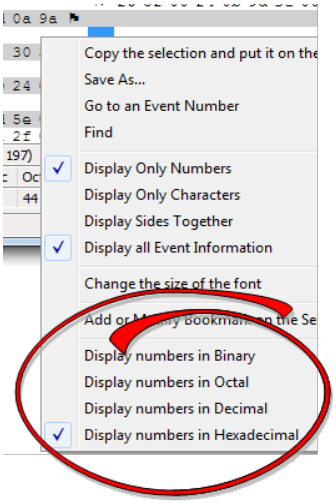


Figure 4.17 - Data display right click menu

If you want to see only the numerical values, click on the **Numbers Only** icon on the **Event Display** toolbar.

4.3.7.3 Switching Between ASCII, EBCDIC, and Baudot

On the **Event Display** window, the analyzer displays data in ASCII by default when you click on the **Characters Only** icon . There are several ways to change the character set used to display data.

1. Go to the **Format** menu and select the character set you want. A check mark next to the character set indicates which set is currently being used.
2. With the data displayed in characters, right-click on the data panel header label to choose a different character set.

If you want to see only characters, click on the Characters Only icon on the Event Display toolbar.

4.3.7.4 Selecting Mixed Channel/Sides

If you want to get more data on the **Event Display** window, you can switch to mixed sides mode. This mode puts all the data together on the same line. Data from one side (**Slave**) is shown on a white background and data from the other side (**Master**)is shown on a gray background.

1. Click once on the **Mixed Sides** icon to put the display in mixed sides mode.
2. Click again to return to side over side mode.
3. You can right click in the center of the data display window to change between mixed and side over side modes by selecting **Display Sides Together**. A check mark is displayed. Click on **Display Sides Together** to remove the check mark and return to side-by-side display.
4. Right click in the sides panel on the right of the data display and select **Display Sides Together**. A check mark is displayed. Click on **Display Sides Together** to remove the check mark and return to side-by-side display.

4.3.7.5 List of all Event Symbols

By default, the **Event Display** shows all events**events**[1], which includes control signal changes, start and end of frame characters and flow control changes. If you want to see only the data bytes, click on the All Events button . Click again to display all events.

Click on a symbol, and the analyzer displays the symbol name and sometimes additional information in the status lines at the bottom of the **Event Display** window. For example, clicking on a control signal change symbol displays which signal(s) changed.

In addition to data bytes, the events shown are (in alphabetical order):

Table 4.3 - Event Symbols

Symbol	Event
	Abort
	Broken Frame - The frame did not end when the analyzer expected it to. This occurs most often with protocols where the framing is indicated by a specific character, control signal change, or other data related event.
	Buffer Overflow - Indicates a buffer overflow error. A buffer overflow always causes a broken frame.
	Control Signal Change - One or more control signals changed state. Click on the symbol, and the analyzer displays which signal(s) changed at the bottom of the Event Display window.
	Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.
	Data Capture Resumed - The Pause icon was clicked again, resuming data capture.
	Dropped Frames - Some number of frames were lost. Click on the symbol, and the analyzer displays many frames were lost at the bottom of the Event Display window.
	End of Frame - Marks the end of a frame.

[1]An event is anything that happens on the circuit or which affects data capture. Data bytes, control signal changes, and long and short breaks are all events, as are I/O Settings changes and Data Capture Paused and Resumed.

Table 4.3 - Event Symbols (continued)

Symbol	Event
	Flow Control Active - An event occurred which caused flow control to become active (i.e. caused the analyzer to stop transmitting data) Events which activate flow control are signal changes or the receipt of an XON character.
	Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. caused the analyzer to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.
	Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.
≠	I/O Settings Change - A change was made in the I/O Settings window which altered the baud, parity, or other circuit setting.
	Long Break
	Low Power - The battery in the ComProbe® is low.
	Short Break
	SPY Event (SPY Mode only) - SPY events are commands sent by the application being spied on to the UART.
	Start of Frame - Marks the start of a frame.
	Begin Sync Character Strip
	End Sync Character Strip
	Sync Dropped
	Sync Found
	Sync Hunt Entered
	Sync Lost
	Test Device Stopped Responding - The analyzer lost contact with the ComProbe for some reason, often because there is no power to the ComProbe.
	Test Device Began Responding - The analyzer regained contact with the ComProbe.
	Timestamping Disabled - Timestamping was turned off. Events following this event are not timestamped.
	Timestamping Enabled - Timestamping was turned on. Events following this event have timestamps.
	Truncated Frame- A frame that is not the same size as indicated within its protocol.
	Underrun Error

Table 4.3 - Event Symbols (continued)

Symbol	Event
	Unknown Event

4.3.7.6 Font Size

The font size can be changed on several **Event Display** windows. Changing the font size on one window does not affect the font size on any other window.

To change the font size:

1. Click on **Event Display** menu **Options,** and select **Change the Font Size**.

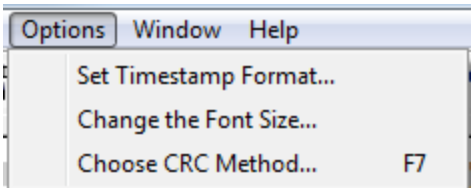


Figure 4.18 - Event Display Options menu

2. Choose a font size from the list.

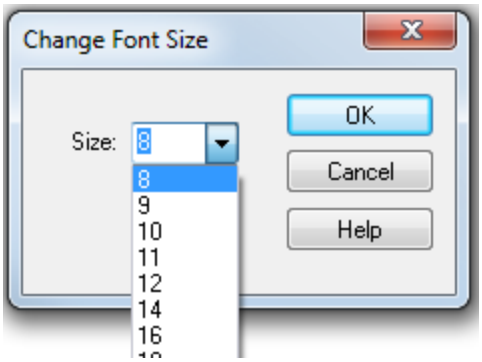


Figure 4.19 - Event Display Font Size Selection

3. Click **OK**.

4.4 Analyzing Protocol Decodes

4.4.1 Frame Display Window

To open this window

Click the **Frame Display** icon on the **Control** window toolbar, or select **Frame Display** from the **View** menu.

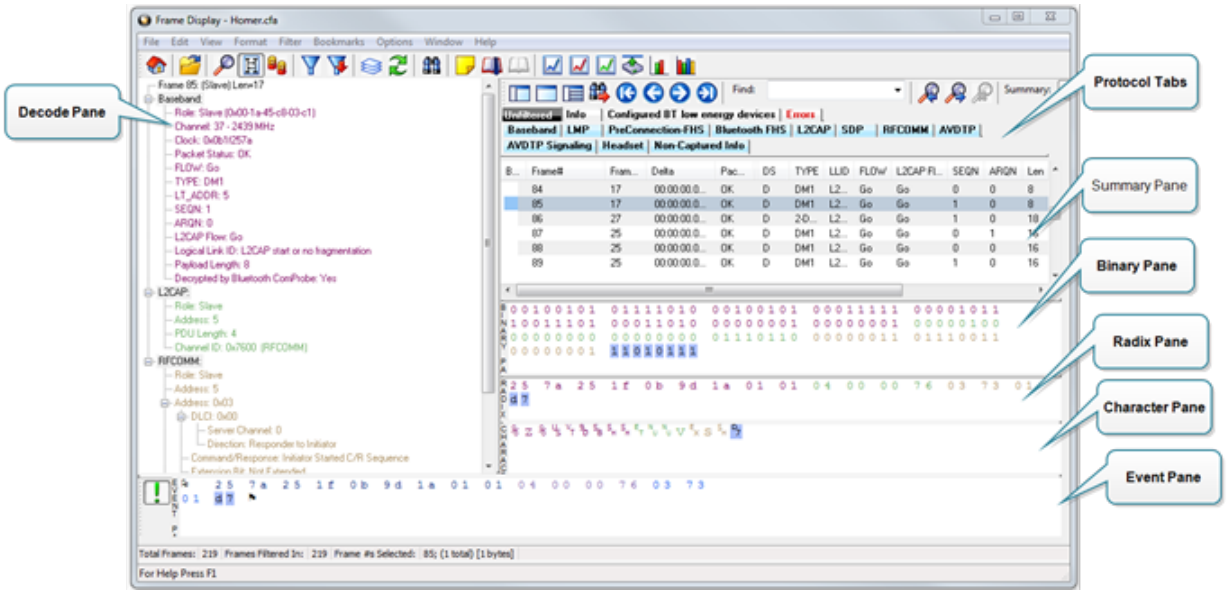


Figure 4.20 - Frame Display with all panes active

Frame Display Panes

The **Frame Display** window is used to view all frame related information. It is composed of a number of different sections or "panes", where each pane shows a different type of information about a frame.

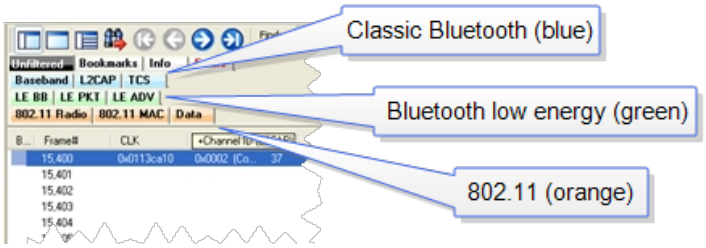
- Summary Pane - The **Summary Pane** displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.
- Decode Pane - The **Decode Pane** displays a detailed decode of the highlighted frame. Fields selected in the **Decode Pane** have the appropriate bit(s) or byte(s) selected in the **Radix**, **Binary**, **Character** , and **Event** panes
- Radix Pane - The **Radix Pane** displays the logical data bytes in the selected frame in either hexadecimal, decimal or octal.
- Binary Pane - The **Binary Pane** displays a binary representation of the logical data bytes.
- Character Pane - The **Character Pane** displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.
- Event Pane - The Event Pane displays the physical data bytes in the frame, as received on the network.

By default, all panes except the **Event Pane** are displayed when the Frame Display is first opened.

Protocol Tabs

Protocol filter tabs are displayed in the **Frame Display** above the Summary pane.

- These tabs are arranged in separate color-coded groups. These groups and their colors are General (white), Classic Bluetooth (blue), Bluetooth low energy (green), 802.11 (orange), USB (purple), NFC (brown) and SD (teal). The General group applies to all technologies. The other groups are technology-specific.



- Clicking on a protocol filter tab in the General group filters in all packets containing that protocol regardless of each packet's technology.
- Clicking on a protocol filter tab in a technology-specific group filters in all packets containing that protocol on that technology.
- A protocol filter tab appears in the General group only if the protocol occurs in more than one of the technology-specific tab groups. For example, if L2CAP occurs in both Classic Bluetooth and Bluetooth low energy , there will be L2CAP tabs in the General group, the Classic Bluetooth group, and the Bluetooth low energy group.

Select the **Unfiltered** tab to display all packets.

There are several special tabs that appear in the **Summary Pane** when certain conditions are met. These tabs appear only in the General group and apply to all technologies. The tabs are:

- **Bookmarks** appear when a bookmark is first seen.
- **Errors** appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- **Info** appears when a frame containing an Information field is first seen.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

Comparing Frames

If you need to compare frames, you can open additional **Frame Display** windows by clicking on the **Duplicate View** icon . You can have as many **Frame Display** windows open at a time as you wish.

Frame Wrapping and Display

In order to assure that the data you are seeing in **Frame Display** are current, the following messages appear describing the state of the data as it is being captured.

- All **Frame Display** panes except the Summary pane display "No frame selected" when the selected frame is in the buffer (i.e. not wrapped out) but not accessible in the **Summary** pane. This can happen when a tab is selected that doesn't filter in the selected frame.
- When the selected frame wraps out (regardless of whether it was accessible in the Summary pane) all **Frame Display** panes except the **Summary** pane display "Frame wrapped out of buffer".

- When the selected frame is still being captured, all **Frame Display** panes except the Summary pane display "Frame incomplete".

4.4.1.1 Frame Display Toolbar

The buttons that appear in the **Frame Display** window vary according to the particular configuration of the analyzer. For controls not available the icons will be grayed-out.

Table 4.4 - Frame Display Toolbar Icons

Icon	Description
	Control – Brings the Control window to the front.
	Open File - Opens a capture file.
	I/O Settings - Opens the I/O Settings dialog.
	Start Capture - Begins data capture to a user designated file.
	Stop Capture - Closes a capture file and stops data capture to disk.
	Save - Save the currently selected bytes or the entire buffer to file.
	Clear- Discards the temporary file and clears the display.
	Event Display – Brings the Event Display window to the front.
	Show Statistics - Opens Statistics dialog
	Duplicate View - Creates a second Frame Display window identical to the first.
	Apply/Modify Display Filters - Opens the Display Filter dialog.
	Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.
	Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data

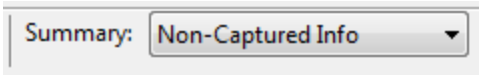
Table 4.4 - Frame Display Toolbar Icons(continued)

Icon	Description
	Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.
	Find - Search for errors, string patterns, special events and more.
	Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.
	Add/Modify Bookmark - Add a new or modify an existing bookmark.
	Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.
	Coexistence View - Opens the Coexistence View
	Extract Data - Opens the Extract Data dialog.
	Audio Extraction - Opens the Audio Extraction dialog.
	Pie Chart - This icon displays a chart that displays the number of frames with and without errors.
Reload Decoders - When **Reload Decoders** is clicked, the plug-ins are reset and received frames are re-decoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.	
	Filter: Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a ToolTip pops up with the full text of the filter.

Table 4.4 - Frame Display Toolbar Icons(continued)

Icon	Description
The following icons all change how the panes are arranged on the Frame Display. Additional layouts are listed in the View menu.	
	Show Default Panes - Returns the panes to their default settings.
	Show Only Summary Pane - Displays only the Summary pane.
	Shall All Panes Except Event Pane - Makes the Decode pane taller and the Summary pane narrower.
	Toggle Display Lock - Prevents the display from updating.
	Go To Frame
	First Frame - Moves to the first frame in the buffer.
	Previous Frame - Moves to the previous frame in the buffer.
	Next Frame - Moves to the next frame in the buffer.
	Last Frame - Moves to the last frame in the buffer.
	Find on Frame Display only searches the Decode Pane for a value you enter in the text box.
	Find Previous Occurrence - Moves to the previous occurrence of the value in the Frame Display Find.
	Find Next Occurrence - Moves to the next occurrence of the value in the Frame Display Find.
	Cancel Current Search - Stops the current Frame Display Find.

Table 4.4 - Frame Display Toolbar Icons(continued)

Icon	Description
Summary:	Summary Drop Down Box: Lists all the protocols found in the data in the file. This box does not list all the protocol decoders available to the analyzer, merely the protocols found in the data. Selecting a protocol from the list changes the Summary pane to display summary information for that protocol. When a low energy predefined Named Filter (like Nulls and Polls) is selected, the Summary drop-down is disabled. 
Text with Protocol Stack: To the right of the Summary Layer box is some text giving the protocol stack currently in use.	

Note: If the frames are sorted in other than ascending frame number order, the order of the frames in the buffer is the sorted order. Therefore the last frame in the buffer may not have the last frame number.

4.4.1.2 Frame Display Status Bar

The **Frame Display Status** bar appears at the bottom of the **Frame Display**. It contains the following information:

- **Frame #s Selected**: Displays the frame number or numbers of selected (highlighted) frames, and the total number of selected frames in parentheses
- **Total Frames**: The total number of frames in the capture buffer or capture file in real-time
- **Frames Filtered In**: The total number of frames displayed in the filtered results from user applied filters in real-time

4.4.1.3 Hiding and Revealing Protocol Layers in the Frame Display

Hiding protocol layers refers to the ability to prevent a layer from being displayed on the **Decode** pane. Hidden layers remain hidden for every frame where the layer is present, and can be revealed again at any time. You can hide as many layers as you wish.

Note: Hiding from the **Frame Display** affects only the data shown in the **Frame Display** and not any information in any other window.

There are two ways to hide a layer.

1. Right-click on the layer in the **Decode** pane, and choose **Hide** [protocol name] **Layer In All Frames**.
2. Click the **Set Protocol Filtering** button on the **Summary** pane toolbar. In the **Protocols to Hide** box on the right, check the protocol layer(s) you want hidden. Click **OK** when finished.

To reveal a hidden protocol layer:

1. Right-click anywhere in the **Decode** pane
2. Choose **Show** [protocol name] **Layer** from the right-click menu, or click the S**et Protocol Filtering** button and un-check the layer or layers you want revealed.

4.4.1.4 Physical vs. Logical Byte Display

The **Event Display** window and **Event Pane** in the **Frame Display** window show the physical bytes. In other words, they show the actual data as it appeared on the circuit. The Radix, Binary and Character panes in the Frame Display window show the logical data, or the resulting byte values after escape codes or other character altering codes have been applied (a process called transformation).

As an example, bytes with a value of less than 0x20 (the 0x indicates a hexadecimal value) cannot be transmitted in Async PPP. To get around this, a 0x7d is transmitted before the byte. The 0x7d says to take the next byte and subtract 0x20 to obtain the true value. In this situation, the Event pane displays 0x7d 0x23, while the Radix pane displays 0x03.

4.4.1.5 Sorting Frames

By default, frames are sorted in ascending numerical sequence by frame number. Click on a column header in the **Summary** pane to sort the frames by that column. For example, to sort the frames by size, click on the **Frame Size** column header.

An embossed triangle next to the header name indicates which column the frames are sorted by. The direction of the triangle indicates whether the frames are in ascending or descending order, with up being ascending.

Note that it may take some time to sort large numbers of frames.

4.4.1.6 Frame Display - Find

Frame Display has a simple **Find** function that you can use to search the Decode Pane for any alpha numeric value. This functionality is in addition to the more robust Search/Find dialog.

Frame Display Find is located below the toolbar on the **Frame Display** dialog.

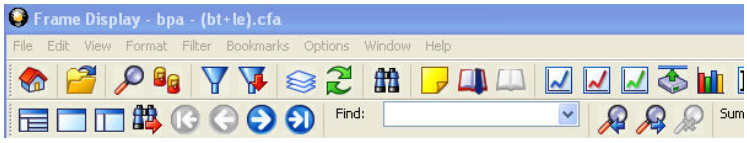


Figure 4.21 - Frame Display Find text entry field

Where the more powerful Search/Find functionality searches the **Decode**, **Binary**, **Radix**, and **Character** panes on **Frame Display** using TImestamps, Special Events, Bookmarks, Patterns, etc.,

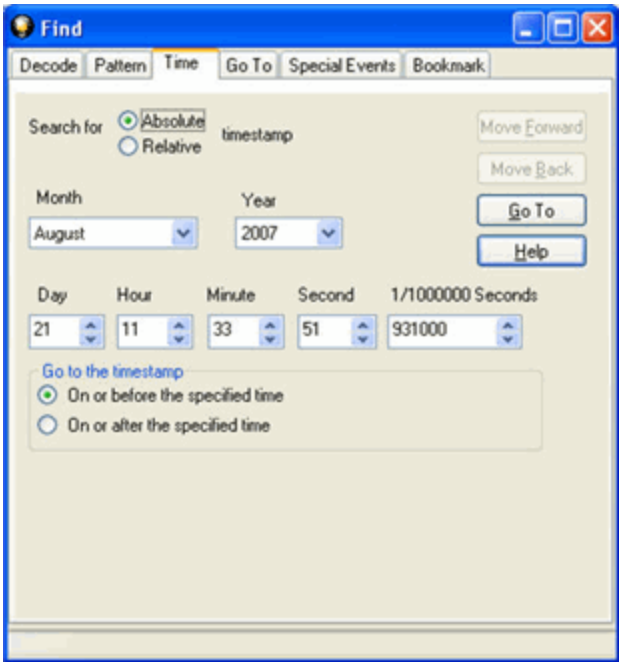


Figure 4.22 - Search/Find Dialog

Find on **Frame Display** only searches the Decode Pane for a value you enter in the text box.

To use **Find**:

1. Select the frame where you want to begin the search.

2. Enter a value in the **Find** text box.

Note: Note: The text box is disabled during a live capture.

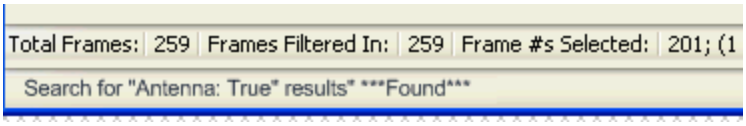
Select **Find Previous Occurrence** to begin the search on frames prior to the frame you selected, or **Find Next Occurrence** to begin the search on frames following the frame you selected.

The next occurrence of the value (if it is found) will be highlighted in the Decode Pane.

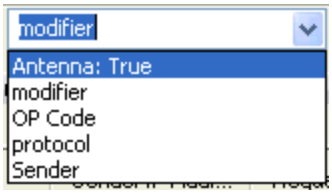
4. Select **Find Previous Occurrence** or **Find Next Occurrence** to continue the search.

There are several important concepts to remember with Find.

- When you enter a search string and select Enter, the search moves forward.
- If you select **Find Previous Occurrence**, when the search reaches the first frame it will then cycle to the last frame and continue until it reaches the frame where the search began.
- Shift + F3 is a shortcut for Find Previous Occurrence.
- If you select **Find Next Occurrence**, when the search reaches the last frame it will then cycle to the first frame and continue until it reaches the frame where the search began.
- F3 is a shortcut for Find Next Occurrence.
- You cannot search while data is being captured.
- After a capture is completed, you cannot search until Frame Display has finished decoding the frames.
- Find is not case sensitive.
- The status of the search is displayed at the bottom of the dialog.
- The search occurs only on the protocol layer selected.
- To search across all the protocols on the Frame Display, select the Unfiltered tab.



- A drop-down list displays the search values entered during the current session of Frame Display.
- The search is cancelled when you select a different protocol tab during a search.
- You can cancel the search at any time by selecting the **Cancel Current Search** button.



4.4.1.7 Synchronizing the Event and Frame Displays

The **Frame Display** is synchronized with the **Event Display.** Click on a frame in the **Frame Display** and the corresponding bytes is highlighted in the **Event Display**. Each **Frame Display** has its own **Event Display**.

As an example, here's what happens if the following sequence of events occurs.

1. Click on the **Frame Display** icon in **Control** window toolbar to open the **Frame Display.**
2. Click on the **Duplicate View** icon to create **Frame Display** #2.
3. Click on **Event Display** icon in **Frame Display** #2. **Event Display** #2 opens. This **Event Display** is labeled #2, even though there is no original **Event Display**, to indicate that it is synchronized with **Frame Display** #2.
4. Click on a frame in **Frame Display** #2. The corresponding bytes are highlighted in **Event Display** #2.
5. Click on a frame in the original **Frame Display**. **Event Display** #2 does not change.

4.4.1.8 Working with Multiple Frame Displays

Multiple Frame Displays are useful for comparing two frames side by side. They are also useful for comparing all frames against a filtered subset or two filtered subsets against each other.

- To create a second Frame Display, click the **Duplicate View** icon on the **Frame Display** toolbar.

  This creates another **Frame Display** window. You can have as many **Frame Displays** open as you wish. Each **Frame Display** is given a number in the title bar to distinguish it from the others.

- To navigate between multiple Frame Displays, click on the **Frame Display** icon in the Control window toolbar.

  A drop-down list appears, listing all the currently open Frame Displays.

- Select the one you want from the list and it comes to the front.

Note: When you create a filter in one **Frame Display**, that filter does not automatically appear in the other **Frame Display**. You must use the Hide/Reveal feature to display a filter created in one Frame Display in another.

Note: When you have multiple **Frame Display** windows open and you are capturing data, you may receive an error message declaring that "Filtering cannot be done while receiving data this fast." If this occurs, you may have to stop filtering until the data is captured.

4.4.1.9 Working with Panes on Frame Display

When the **Frame Display** first opens, all panes are displayed except the **Event** pane (To view all the panes, select **Show All Panes** from the **View** menu).

- The **Toggle Expand Decode Pane** icon makes the decode pane longer to view lengthy decodes better.
- The **Show Default Panes** icon returns the **Frame Display** to its default settings.
- The Show only Summary Pane icon displays on the Summary Pane.

To close a pane, right-click on the pane and select **Hide This Pane** from the pop-up menu, or de-select **Show [Pane Name]** from the **View** menu.

To open a pane, right-click on the any pane and select **Show Hidden Panes** from the pop-up menu and select the pane from the fly-out menu, or select **Show [Pane Name]** from the **View** menu.

To re-size a pane, place the cursor over the pane border until a double-arrow cursor appears. Click and drag on the pane border to re-size the pane.

4.4.1.10 Frame Display - Byte Export

The captured frames can be exported as raw bytes to a text file.

1. From the **Frame Display File** menu select **Byte Export...**.

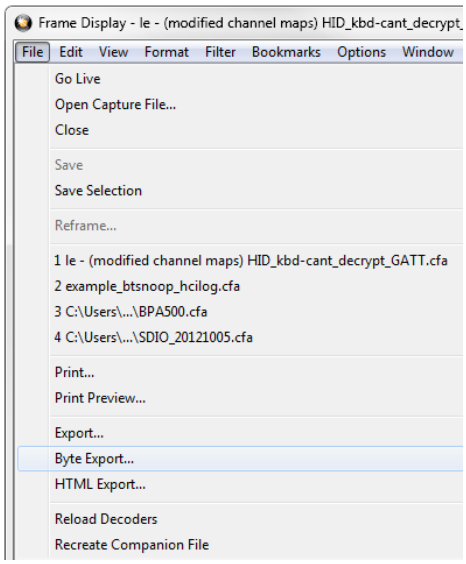


Figure 4.23 - Frame Display File menu, Byte Export

2. From the Byte Export window specify the frames to export.

   - All Frames exports all filtered-in frames including those scrolled off the **Summary** pane. Filtered-in frames are dependent on the selected **Filter** tab above the **Summary** pane. Filtered-out frames are not exported.
   - Selected Frames export is the same as **All Frames** export except that only frames selected in the **Summary** pane will be exported.

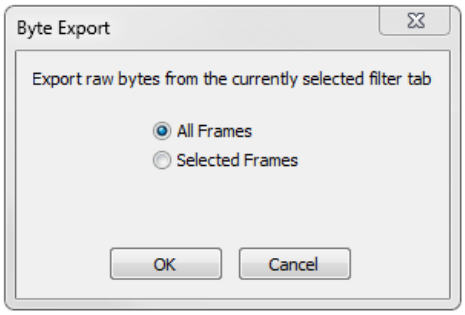


Figure 4.24 - Byte Export dialog

   Click the **OK** button to save the export. Clicking the **Cancel** button will exit Byte Export.

3. The **Save As** dialog will open. Select a directory location and enter a file name for the exported frames file.

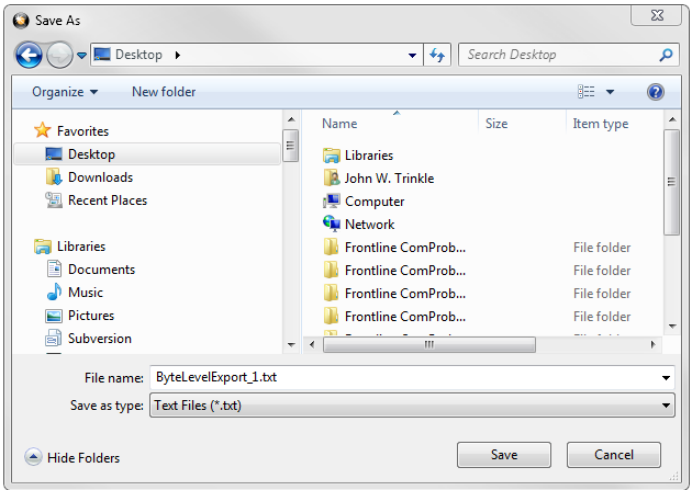


Figure 4.25 - Save As dialog

Click on the **Save** button.

The exported frames are in a text file that can be opened in any standard text editing application. The header shows the export type, the capture file name, the selected filter tab, and the number of frames. The body shows the frame number, the timestamp in the same format shown in the **Frame Display Summary** pane, and the frame contents as raw bytes.

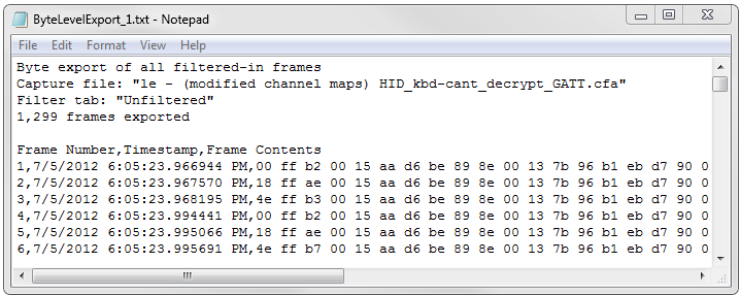

ByteLevelExport_1.txt - Notepad
File Edit Format View Help
Byte export of all filtered-in frames
Capture file: "le - (modified channel maps) HID_kbd-cant_decrypt_GATT.cfa"
Filter tab: "Unfiltered"
1,299 frames exported
Frame Number,Timestamp,Frame Contents
1,7/5/2012 6:05:23.966944 PM,00 ff b2 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
2,7/5/2012 6:05:23.967570 PM,18 ff ae 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
3,7/5/2012 6:05:23.968195 PM,4e ff b3 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
4,7/5/2012 6:05:23.994441 PM,00 ff b2 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
5,7/5/2012 6:05:23.995066 PM,18 ff ae 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0
6,7/5/2012 6:05:23.995691 PM,4e ff b7 00 15 aa d6 be 89 8e 00 13 7b 96 b1 eb d7 90 0

Figure 4.26 - Sample Exported Frames Text File

4.4.1.11 Panes in the Frame Display

4.4.1.11.1 Summary Pane

The **Summary** pane displays a one-line summary of every frame in a capture buffer or file, including frame number, timestamp, length and basic protocol information. The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

On a two-channel circuit, the background color of the one-line summary indicates whether the frame came from the DTE or the DCE device. Frames with a white background come from the DTE device, frames with a gray background come from the DCE device.

The ComProbe USB **Summary** pane in displays a one-line summary of every transaction in a capture buffer or

file. Whenever there is a transaction it is shown on a single line instead of showing the separate messages that comprise the transaction. The **Msg** column in that case says “Transaction”.

Each message in a transaction contains a packet identifier (PID). All of the PIDs in a transaction are shown in the transaction line.

All "IN" transactions (i.e. transactions that contain an IN token message) are shown with a purple background. All other transactions and all non-transactions are shown with a white background. "IN" transactions have special coloring because that is the only place where the primary data flow is from a device to the Host.

The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

Frame numbers in red indicate errors, either physical (byte-level) or frame errors. If the error is a frame error in the displayed protocol layer, the bytes where the error occurred is displayed in red. The Decode Pane gives precise information as to the type of error and where it occurred.

The **Summary** pane is synchronized with the other panes in this window. Click on a frame in the **Summary** pane, and the bytes for that frame is highlighted in the **Event** pane while the **Decode** pane displays the full decode for that frame. Any other panes which are being viewed are updated accordingly. If you use one pane to select a subset of the frame, then only that subset of the frame is highlighted in the other panes.

Protocol Tabs

Protocol filter tabs are displayed in the Frame Display above the Summary pane.

- These tabs are arranged in separate color-coded groups. These groups and their colors are General (white), Classic Bluetooth® (blue), *Bluetooth* low energy (green), 802.11 (orange), USB (purple), and SD (brown). The General group applies to all technologies. The other groups are technology-specific.

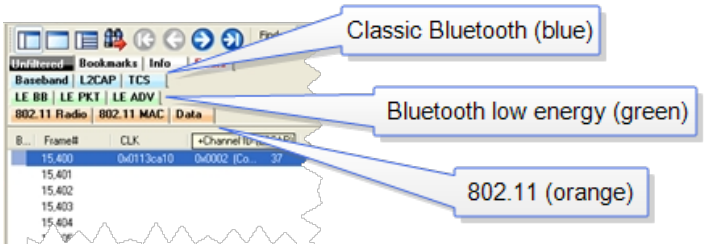


Figure 4.27 - Example Protocol Tags

- Clicking on a protocol filter tab in the General group filters in all packets containing that protocol regardless of each packet’s technology.
- Clicking on a protocol filter tab in a technology-specific group filters in all packets containing that protocol on that technology.
- A protocol filter tab appears in the General group only if the protocol occurs in more than one of the technology-specific tab groups. For example, if L2CAP occurs in both Classic *Bluetooth* and *Bluetooth* low energy , there will be L2CAP tabs in the General group, the Classic *Bluetooth* group, and the *Bluetooth* low energy group.

Select the Unfiltered tab to display all packets.

There are several special tabs that appear in the **Summary** pane when certain conditions are met. These tabs appear only in the General group and apply to all technologies. The tabs are:

- **Bookmarks** appear when a bookmark is first seen.
- **Errors** appear when an error is first seen. An error is a physical error in a data byte or an error in the protocol decode.
- **Info** appears when a frame containing an Information field is first seen.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

The tabs disappear when the capture buffer is cleared during live capture or when decoders are reloaded, even if one of the tabs is currently selected. They subsequently reappear as the corresponding events are detected.

Use the navigation icons, keyboard or mouse to move through the frames. The icons and move you to the first and last frames in the buffer, respectively. Use the Go To icon to move to a specific frame number.

Placing the mouse pointer on a summary pane header with truncated text displays a tooltip showing the full header text.

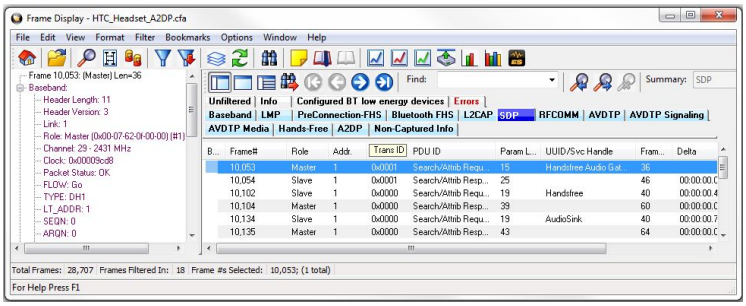

Frame Display - HTC_Headset_A2DP.cfa
File Edit View Format Filter Bookmarks Options Window Help
Unfiltered | Info | Configured BT low energy devices | Errors
Baseband | LMP | PreConnection-FHS | Bluetooth FHS | L2CAP | SDP | RFCOMM | AVDTP | AVDTP Signaling
AVDTP Media | Hands-Free | A2DP | Non-Captured Info
Trans ID
PDU ID
Total Frames: 28,707 Frames Filtered In: 18 Frame #s Selected: 10,053; (1 total)
For Help Press F1

Figure 4.28 - Summary pane (right) with Tooltip on Column 5 (Tran ID)

Sides in *Bluetooth* low energy

A Bluetooth low energy data connection consists of connection events, which are a series of transmissions on the same channel. In each connection event the master transmits first, then the slave, and then the devices take turns until the connection event is finished.

When the data connection is encrypted and the packets are successfully decrypted, the sniffer can determine exactly who sent which packet (only non-empty, encrypted packets – empty packets are never encrypted). These packets are labeled either 'M' for master or 'S' for slave.

When the data connection is unencrypted or when encrypted packets are not successfully decrypted by the sniffer, the sniffer cannot distinguish the two devices' (master and slave) packets by their content, just by the packet timing. In those cases we label each device as side '1' or '2', not as master or slave. In each connection event, packets sent by the device which transmitted first in the connection event are labeled '1', and packets sent by the device which transmitted second are labeled '2'.

If no packets in the connection event are missed by the sniffer, the device labeled '1' is the master and the device labeled '2' is the slave. However, if we do not capture the very first packet in a connection event (i.e. the packet sent by the master) but do capture the packet sent by the slave, we label the slave as side '1' since it is the first device we heard in the connection event. Because there is potential clock drift since the last connection event,

we cannot use the absolute timing to correct this error; there would still be cases where we get it wrong. Therefore we always assign '1' to the first packet in a connection event. So even though it is rare, there are connection events where packets sent by the slave device are labeled '1' and packets sent by the master are labeled '2'.

Finally, in a noisy environment it is also possible that the sniffer does not capture packets in the middle of a connection event. If this occurs and the sniffer cannot determine the side for the remaining packets in that connection event, the side is labeled 'U' for "unknown".

4.4.1.11.2 Customizing Fields in the Summary Pane

You can modify the **Summary** Pane in **Frame Display**.

Summary pane columns can be reordered by dragging any column to a different position.

Fields from the **Decode** pane can be added to the summary pane by dragging any **Decode**pane field to the desired location in the **summary** pane header. If the new field is from a different layer than the summary pane a plus sign (+) is prepended to the field name and the layer name is added in parentheses. The same field can be added more than once if desired, thus making it possible to put the same field at the front and back (for example) of a long header line so that the field is visible regardless of where the header is scrolled to.

An added field can be removed from the **Summary** pane by selecting **Remove New Column** from the right-click menu.

The default column layout (both membership and order) can be restored by selecting **Restore Default Columns** from the **Format** or right-click menus.

Changing Column Widths

To change the width of a column:

1. Place the cursor over the right column divider until the cursor changes to a solid double arrow.
2. Click and drag the divider to the desired width.
3. To auto-size the columns, double-click on the column dividers.

Hiding Columns

To hide a column:

1. Drag the right divider of the column all the way to the left.
2. The cursor changes to a split double arrow when a hidden column is present.
3. To show the hidden column, place the cursor over the divider until it changes to a split double arrow, then click and drag the cursor to the right.
4. The **Frame Size**, **Timestamp**, and **Delta** columns can be hidden by right-clicking on the header and selecting **Show Frame Size Column, Show Timestamp Column,** or **Show Delta Column**. Follow the same procedure to display the columns again.

Moving Columns - Changing Column Order

To move a column :

1. Click and hold on the column header
2. Drag the mouse over the header row.
3. A small white triangle indicates where the column is moved to.
4. When the triangle is in the desired location, release the mouse.

Restoring Default Column Settings

To restore columns to their default locations, their default widths, and show any hidden columns

1. Right-click on any column header and choose **Restore Default Column Widths**, or select **Restore Default Column Widths** from the **Format** menu.

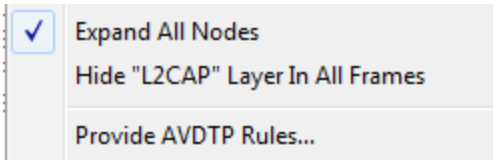
4.4.1.11.3 Frame Symbols in the Summary Pane

Table 4.5 - Frame Symbols

Symbol	Description
	A green dot means the frame was decoded successfully, and the protocol listed in the **Summary Layer** drop-down box exists in the frame. No dot means the frame was decoded successfully, but the protocol listed in the **Summary Layer** drop-down box does not exist in the frame.
	A green circle means the frame was not fully decoded. There are several reasons why this might happen. • One reason is that the frame compiler hasn't caught up to that frame yet. It takes some time for the analyzer to compile and decode frames. Frame compilation also has a lower priority than other tasks, such as capturing data. If the analyzer is busy capturing data, frame compilation may fall behind. When the analyzer catches up, the green circle changes to either a green dot or no dot. • Another reason is if some data in the frame is context dependent and we don't have the context. An example is a compressed header where the first frame gives the complete header, and subsequent frames just give information on what has changed. If the analyzer does not capture the first frame with the complete header, it cannot decode subsequent frames with partial header information.
	A magenta triangle indicates that a bookmark is associated with this frame. Any comments associated with the bookmark appear in the column next to the bookmark symbol.

4.4.1.11.4 Decode Pane

The **Decode** pane (aka detail pane) is a post-process display that provides a detailed decode of each frame transaction (sometimes referred to as a frame). The decode is presented in a layered format that can be expanded and collapsed depending on which layer or layers you are most interested in. Click on the plus sign to expand a layer. The plus sign changes to a minus sign. Click on the minus sign to collapse a layer. **Select Show All** or **Show Layers** from the **Format** menu to expand or collapse all the layers. Layers retain their expanded or collapsed state between frames.



Protocol layers can be hidden, preventing them from being displayed on the **Decode** pane. Right-click on any protocol layer and choose **Hide** [protocol name] from the right-click menu.

In a USB transaction, all messages that comprise the transaction are shown together in the detail pane. The color coding that is

applied to layers when the detail pane displays a single message is applied to both layers and messages when the detail pane displays a transaction. To keep the distinction between layers and messages clear, each header of each message in the detail pane ends with the word “Message” or “Messages”. The latter is used because data and handshake messages are shown as a single color-coded entry

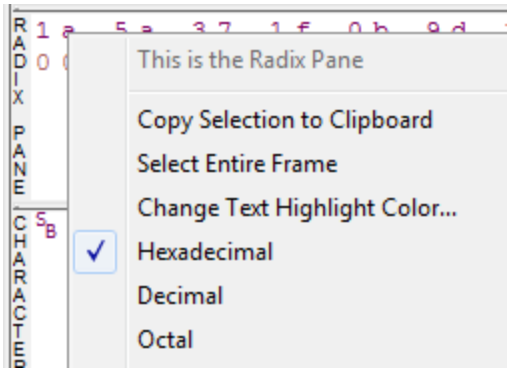
Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the **Event**, **Radix**, **Binary** and **Character** panes. The colors are not assigned to a protocol, but are assigned to the layer.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

Click the **Toggle Expand Decode Pane** icon to make the **Decode** pane taller. This allows for more of a lengthy decode to be viewed without needing to scroll.

4.4.1.11.5 Radix or Hexadecimal Pane

The **Radix** pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the **Format** menu, or by right-clicking on the pane and choosing **Hexadecimal**, **Decimal** or **Octal**.



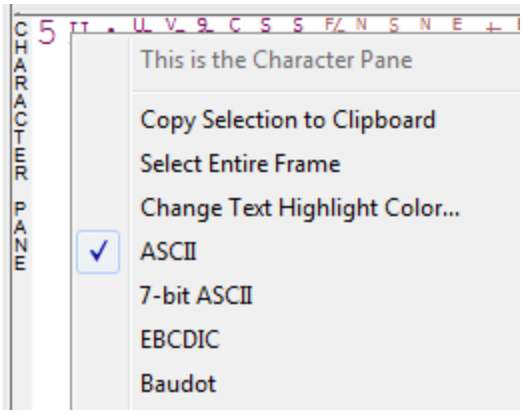
Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.6 Character Pane

The **Character** pane represents the logical bytes in the frame in **ASCII**, **EBCDIC** or **Baudot**. The character set can be changed from the **Format** menu, or by right-clicking on the pane and choosing the appropriate character set.



Because the **Character** pane displays the logical bytes rather than the physical bytes, the data in the **Character** pane may be different from that in the **Event** pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the **Decode** pane.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.7 Binary Pane

The **Binary** pane displays the logical bytes in the frame in binary.

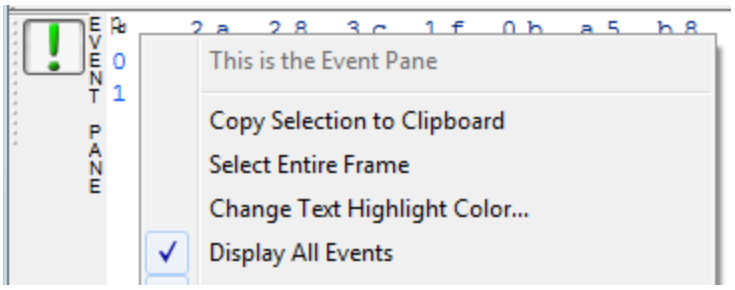
Because the **Binary** pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the **Event** pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the **Decode** pane.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.8 Event Pane

The **Event** pane shows the physical bytes in the frame. You can choose between displaying only the data events or displaying all events by clicking the **All Events** icon .


EVENT PANE
2 a 2 8 3 c 1 f 0 b a 5 b 8
0
1
This is the Event Pane
Copy Selection to Clipboard
Select Entire Frame
Change Text Highlight Color...
Display All Events

Displaying all events means that special events, such as **Start of Frame**, **End of Frame** and any signal change events, are displayed as special symbols within the data.

The status lines at the bottom of the pane give the same information as the status lines in the **Event Display** window. This includes physical data errors, control signal changes (if appropriate), and timestamps.

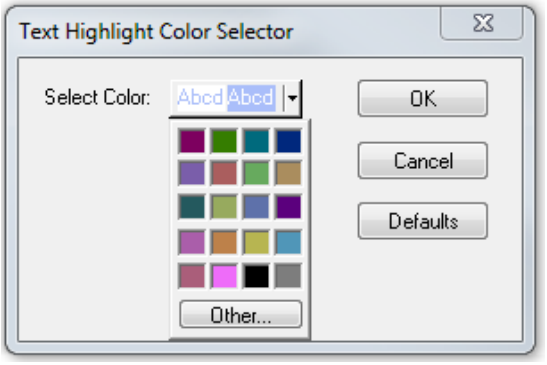
Because the **Event** pane displays the physical bytes rather than the logical bytes, the data in the **Event** pane may be different from that in the **Radix**, **Binary** and **Character** panes. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The **Event**, **Radix**, **Binary**, **Character** and **Decode** panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

4.4.1.11.9 Change Text Highlight Color

Whenever you select text in the **Binary**, **Radix**, or **Character** panes in **Frame Display**, the text is displayed with a highlight color. You can change the color of the highlight.



1. Select **Change Text Highlight Color** from the **Options** menu. You can also access the option by right clicking in any of the panes.
2. Select a color from the drop-down menu.
3. Click **OK**.

The highlight color for the text is changed.

Select **Cancel** to discard any selection. Select **Defaults** to return the highlight color to blue.

4.4.1.12 Protocol Layer Colors

4.4.1.12.1 Data Byte Color Notation

The color of the data in the panes specifies which layer of the protocol stack the data is from. All data from the first layer is bright blue, the data from the second layer is green, the third layer is pink, etc. The protocol name for each layer in the **Decode** pane is in the same color. Note that the colors refer to the layer, not to a specific protocol. In some situations, a protocol may be in two different colors in two different frames, depending on where it is in the stack. You can change the default colors for each layer.

Red is reserved for bytes or frames with errors. In the **Summary** pane, frame numbers in red mean there is an error in the frame. Also, the **Errors** tab is displayed in red. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the **Radix**, **Character**, **Binary** and **Event** panes mean there is a physical error associated with the byte.

4.4.1.12.2 Changing Protocol Layer Colors

You can differentiate different protocol layers in the **Decode**, **Event**, **Radix**, **Binary** and **Character** panes.

1. Choose **Select Protocol Layer Colors** from the **Options** menu to change the colors used.

   The colors for the different layers is displayed.

2. To change a color, click on the arrow next to each layer and select a new color.
3. Select **OK** to accept the color change and return to **Frame** Display.

Select **Cancel** to discard any selection. Select **Defaults** to return the highlight colors to the default settings.

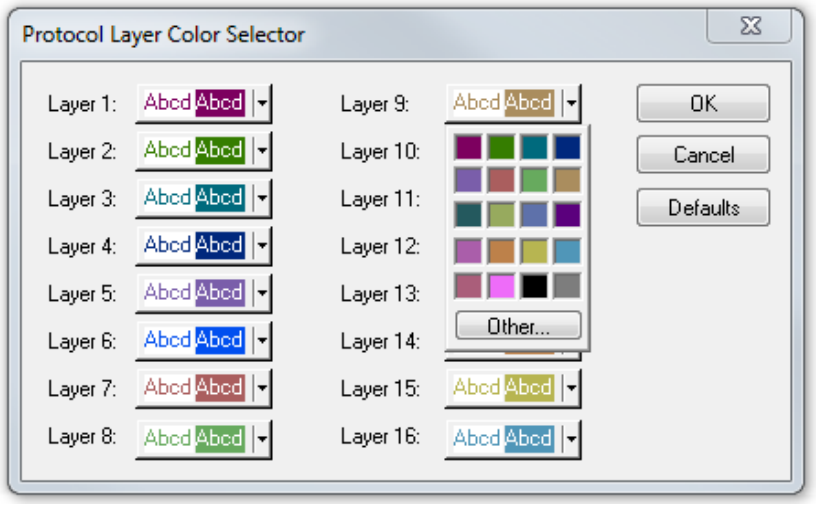


Figure 4.29 - Frame Display Protocol Layer Color Selector

4.4.1.13 Filtering

Filtering allows the user to control the display which capture frames are displayed. Filters fall into two general categories:

1. **Display filters** allow a user to look at a subset of captured data without affecting the capture content. Frames matching the filter criteria appear in the **Frame Display**; frames not matching the criteria will not appear.
2. **Connection filters** Two options are available.
    a. A Bluetooth connection: Displays only the frames associated with a Classic *Bluetooth* link or a *Bluetooth* low energy access address. A new **Frame Display** will open showing only the protocol tabs, frames, summary, and events associated with that particular *Bluetooth* connection.
    b. A specific wireless or wired technology. Displays all of the frames associated with:
        - Classic *Bluetooth*
        - *Bluetooth* low energy
        - 802.11
        - HCI

        A new Frame Display will open showing only the protocol tabs, frames, summary and events associated with the selected technology.

4.4.1.13.1 Display Filters

A display filter looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Display filters allow a user to look at a subset of captured data without affecting the capture content. There are three general classes of display filters:

- Protocol Filters
- Named Filters
- Quick Filter

Protocol Filters

Protocol filters test for the existence of a specific single layer. The system creates a protocol filter for each decoder that is loaded if that layer is encountered in a capture session.

There are also three special purpose filters that are treated as protocol filters:

- All Frames with Errors
- All Frames with Bookmarks
- All Special Information Nodes

Named Filters

- Named filters test for anything other than simple single layer existence. Named filters can be constructed that test for the existence of multiple layers, field values in layers, frame sizes, etc., as well as combinations of those things. Named filters are persistent across sessions.

- Named filters are user-defined. User-defined filters persist in a template file. User defined filters can be deleted.

Quick Filters

- Quick Filters are combinations of Protocol Filters and/or Named Filters that are displayed on the Quick Filter tab.
- Quick Filters cannot be saved and do not persist across sessions.
- Quick Filters are created on the Quick Filter Dialog.

4.4.1.13.1.1 Creating a Display Filter

There are two steps to using a display filter. Define the filter conditions, and then apply the filter to the data set. The system combines both filter definition and application in one dialog.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters** from the **Filter** menu to open the **Set Condition** dialog box. The Set Condition dialog is self configuring which means that when you **Select each frame** under **Conditions** the following displayed fields depend on your selection. With each subsequent selection the dialog fields will change depending on you selection in that field.

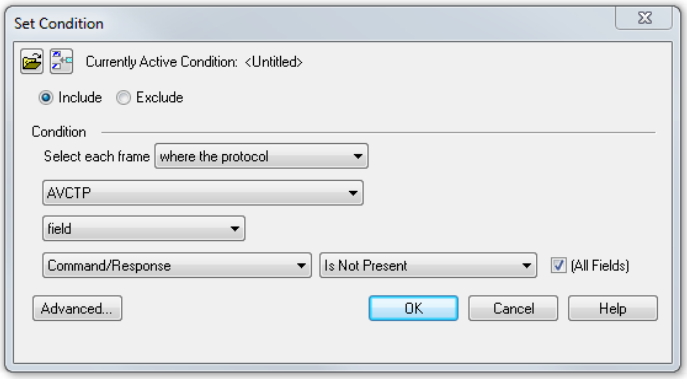


Figure 4.30 - Example: Set Conditions Self Configuring Based on Protocol Selection

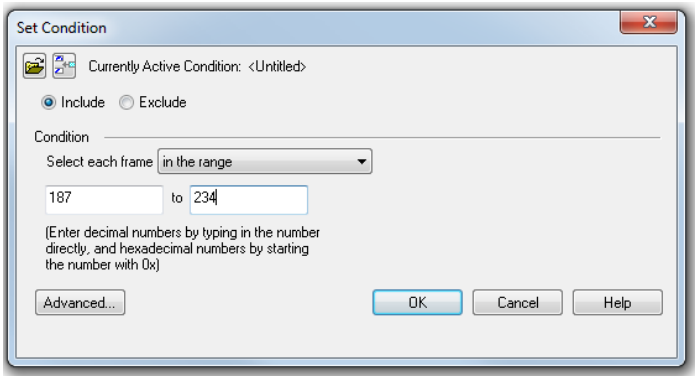


Figure 4.31 - Example: Set Conditions Self Configuring Based on Frame Range

2. Select **Include** or **Exclude** to add filtered data or keep out filtered data respectively.
3. Select the initial condition for the filter from the drop-down list.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the condition statement is complete.
5. Click OK. The system displays the **Save Named Condition** dialog. Provide a name for the filter condition or accept the default name provided by the system and click **OK**. Prohibited characters are left bracket '[', right bracket ']' and equal sign '='. The **Set Condition** dialog box closes, creates a tab on the **Frame Display** with the filter name, and applies the filter.

The filter also appears in the Quick Filtering and Hiding Protocols dialog.

When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Notes:

- The system requires naming and saving of all filters created by the user.
- The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.
- When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other **Frame Display** windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different **Frame Display** window.

4.4.1.13.1.2 Including and Excluding Radio Buttons

All filter dialog boxes contain an **Include** and an **Exclude** radio button. These buttons are mutually exclusive. The **Include**/**Exclude** selection becomes part of the filter definition, and appears as part of the filter description displayed to the right of the Toolbar.

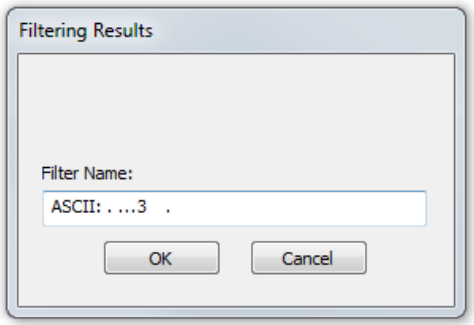
Include: A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

Exclude: A filter constructed with the "Exclude" button selected, returns a data set that excludes frames that meet the conditions defined by the filter and consists of frames that do not.

4.4.1.13.1.3 Named Display Filters

You can create a unique display filter by selecting a data type on the **Frame Display** and using a right click menu. When you create a **Name Filter**, it appears in the Quick Filtering dialog, where you can use it do customize the data you see in the **Frame Display** panes.

1. Select a frame in the **Frame Display Summary** Pane.
2. Right click in the one of the data columns in the **Summary** Pane: CRC, NESN, DS, Packet Success, Ethertype, Source Address, etc.
3. Select **Filter in *(data type)* =** . The **Filtering Results** dialog appears.
4. Enter a name for the filter
5. Select **OK**.



The filter you just created appears in the **Named Filters** section of the Quick Filtering dialog.

4.4.1.13.1.4 Using Compound Display Filters

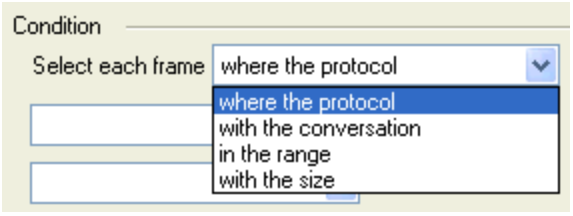
Compound filters use boolean logic to create complex and precise filters. There are three primary Boolean logic operators: **AND**, **OR**, and **NOT**.

The **AND** operator narrows the filter, the **OR** operator broadens the filter, and the **NOT** operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

There are two steps to using a compound filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the filter menu to open the **Set Condition** dialog box.
2. Click the **Advanced** button on the **Set Condition** dialog box.
3. Select **Include** or **Exclude** radio button.

   Now you can set the conditions for the filter.
4. Select the initial condition for the filter from the combo box at the bottom of the dialog for **Select each frame.**
5. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the conditions statement is complete.



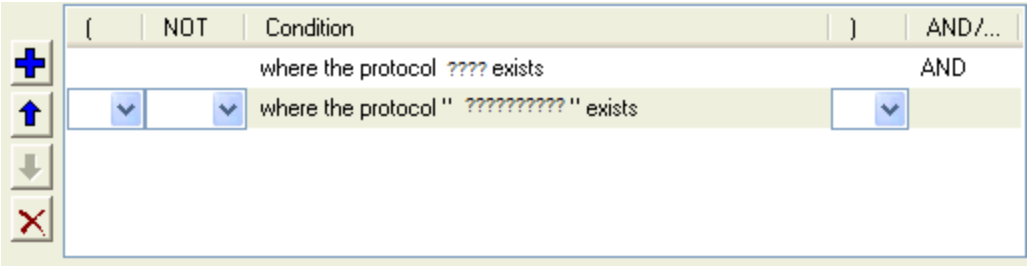


Figure 4.32 - Two Filter Conditions Added with an AND Operator

6. Click the plus icon on the left side of the dialog box and repeat steps 4 and 5 for the next condition. Use the up and down arrow icons on the left side of the dialog box to order your conditions, and the delete button to delete conditions from your filter.
7. Continue adding conditions until your filter is complete.
8. Include parentheses as needed and set the boolean operators.
9. Click **OK**.
10. The system displays the **Save Named Condition** dialog. Provide a name for the filter condition or accept the default name provided by the system and click **OK**.

Figure 4.33 - Save Named Filter Condition Dialog

The **Set Condition** dialog box closes, creates a tab on the **Frame Display** with the filter name, and applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Note: The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.

4.4.1.13.1.5 Defining Node and Conversation Filters

There are two steps to using Node and Conversation display filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the filter menu to open the **Set Condition** dialog box.
2. From the **Select each frame** combo box choose **frames with the conversation** as the initial condition.
3. Select an address type—IP, MAC, TCP/UDB—from the **Type**combo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first **Address** combo box.
5. Choose a direction arrow from the direction box . The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination.

6. If you want to filter on just one node address, skip step 7 and continue with step 8.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select a node address from the second Address combo box..
8. Click **OK**. The **Set Condition** dialog box closes and the analyzer applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Note: The **OK** button is unavailable (grayed out) until the condition selections are complete.

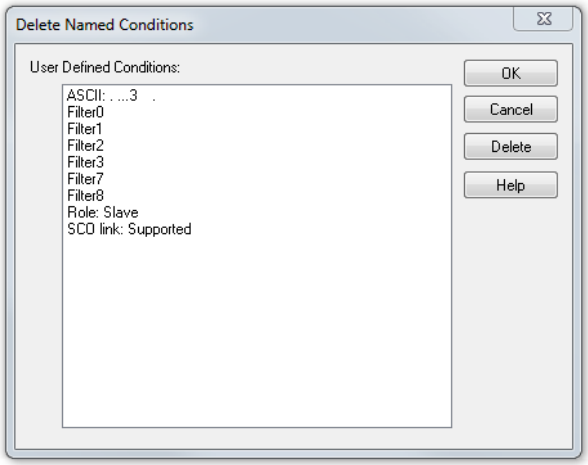
4.4.1.13.1.6 The Difference Between Deleting and Hiding Display Filters

If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

Deleting a saved filter removes the filter from the current session and all subsequent sessions. In order to retrieve a deleted filter, the user must recreate it using the **Set Conditions** dialog.

Hiding a filter merely removes the filter from the display. A hidden filter can be reapplied using the Show/Hide procedure.

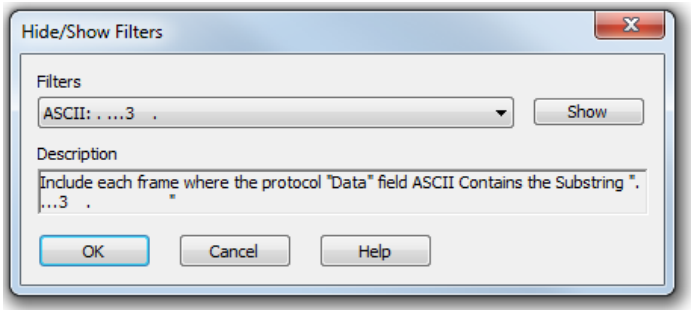
Deleting Saved Display Filters



1. Select **Delete Display Filters** from the **Filter** menu in the **Frame Display** window to open the **Delete Named Condition** dialog. The system displays the **Delete Named Condition** dialog with a list of all user defined filters.
2. Select the filter to be deleted from the list.
3. Click the **Delete** button.
4. Click **OK**. The **Delete Named Condition** dialog box closes and the system deletes the filter.

Hiding and Revealing Display Filters

If a display filter is showing the following steps will hide that filter but will not delete it.



1. **Select Hide/Show Display Filters…** from the **Filter** menu on the **Frame Display** window to open the **Hide/Show Filters** dialog. The system displays the **Hide/Show Filters** dialog with a list of all user defined filters.
2. Select the filter to be hidden from the combo box.
3. Click the **Hide** button. The **Hide** button is only showing if the selected filter is currently showing in the **Frame Display**.
4. Click **OK**. The **Hide/Show Filters** dialog box closes, and the system hides the filter and removes the filter tab from the Frame Display.

If a display filter is hidden the following steps will reveal that filter in the **Frame Display**.

1. Select **Hide/Show Display Filters…** from the **Filter** menu in the **Frame Display** window to open the **Hide/Show Filters** dialog. The system displays the **Hide/Show Filters** dialog with a list of all user defined filters.
2. Select the filter to be revealed from the combo box.
3. Click the **Show** button.
4. Click **OK**. The **Hide/Show Filters** dialog box closes and the system reveals the filter in the **Frame Display**.

You can also open the Quick Filter dialog and check the box next to the hidden filter to show or hide a display filter.

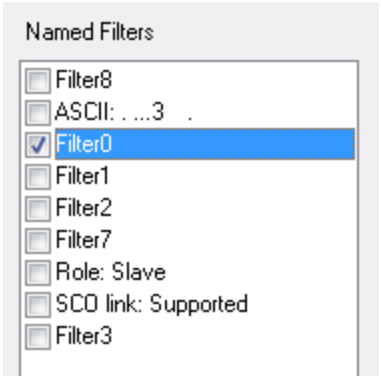


Figure 4.34 - Using Named Filters Section of Quick Filters to Show/Hide Filters

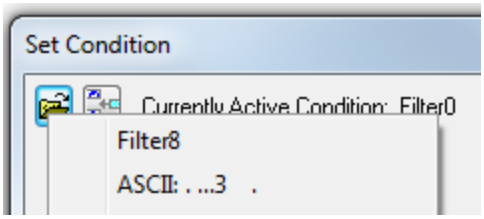
Note: When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Show dialog to display a filter created in one Frame Display in different Frame Display window.

4.4.1.13.1.7 Editing Filters

Modifying a Condition in a Filter

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters...** from the **Filter** menu to open the **Set Condition** dialog box. The **Set Condition** dialog box displays the current filter definition at the top of the dialog.

   To display another filter, click the **Open** icon, and select the filter from the pop-up list of all the saved filters.



2. Edit the desired parameter of the condition: Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested parameters in the fields provided until the condition statement is complete.
3. Click **OK**. The system displays the **Save Named Condition** dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click **OK**. If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click **OK**.) The **Set Condition** dialog box closes, and the system applies the modified filter.

Note: When a display filter is applied, a description of the filter appears to the right of the toolbar in the Frame Display windows.

Note: The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.

Deleting a Condition in a Filter

If a display filter has two or more conditions you can delete conditions. If there is only one condition set in the filter you must delete the filter using **Delete Display Filters...** from the **Filters** menu.

1. Click the **Display Filters** icon on the **Frame Display** window or select **Apply/Modify Display Filters…** from the **Filter** menu to open the **Set Condition** dialog box. Click on the Advanced button to show the condition in Boolean format. The dialog box displays the current filter definition. To display another filter, click the Open icon, and select the filter from the pop-up list of all the saved filters.

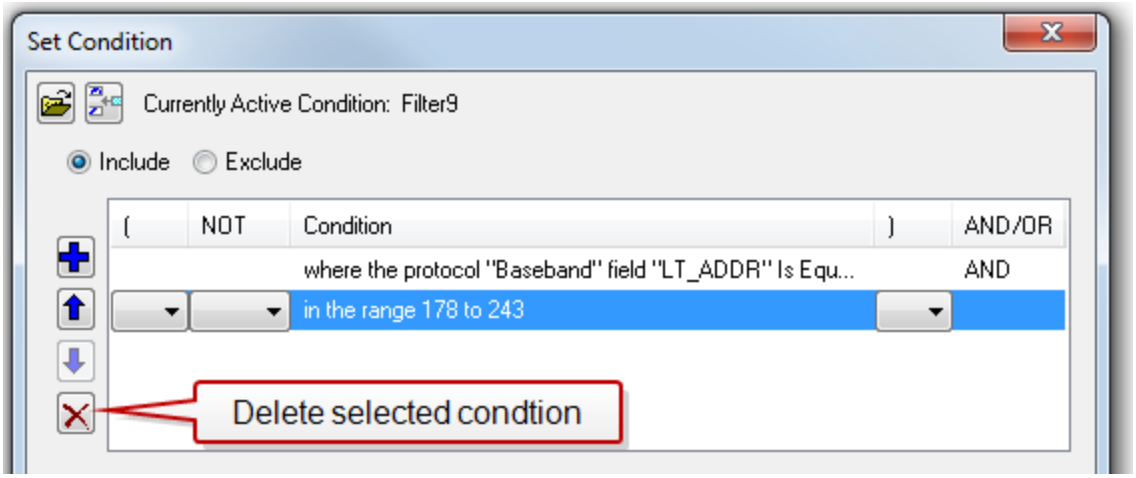


Figure 4.35 - Set Condition Dialog in Advanced View

2. Select the desired condition from the filter definition.
3. Click the **Delete Selected Line** icon.
4. Edit the Boolean operators and parentheses as needed.
5. Click **OK**. The system displays the **Save Named Condition** dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click **OK**. (If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click **OK**.) The **Set Condition** dialog box closes, and the system applies the modified filter.

Note: When a display filter is applied, a description of the filter appears to the right of the toolbar in the **Frame Display** windows.

Note: The **OK** button on the **Set Condition** dialog box is unavailable (grayed out) until the condition selections are complete.

Renaming a Display Filter

1. Select **Rename Display Filters…** from the **Filter** menu in the **Frame Display** window to open the **Rename Filter** dialog. The system displays the **Rename Filter** dialog with a list of all user defined filters in the **Filters** combo box.

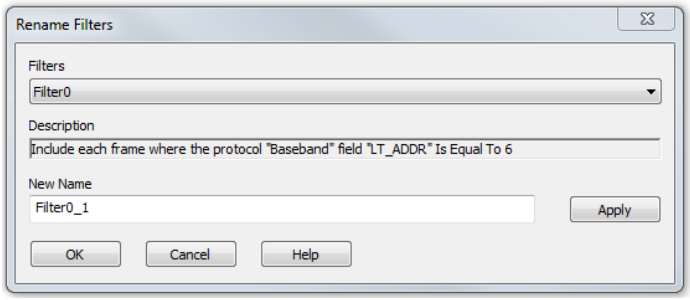


Figure 4.36 - Rename Filters Dialog

2. Select the filter to be renamed from the combo box.
3. Enter a new name for the filter in the **New Name** box. Optionally click the **Apply** button and the new name will appear in the **Filters** combo box and the **New Name** box will empty. This option allows you to rename several filters without closing the **Rename Filter** dialog each time.
4. Click **OK**. The **Rename Filter** dialog box closes and the system renames the filter.

4.4.1.13.2 Connection Filtering

Connection Filtering allows the user to view a subset of the total available packets within the **Frame Display**. The subset can include data from a single *Bluetooth* connection, or all of the BR/EDR packets, all of the low energy packets, all of the 802.11 packets, or all of the HCI packets.

Bluetooth Applicability

A connection (device pair) is identified by

1. A Link for Classic *Bluetooth*,
2. An Access Address for *Bluetooth* low energy.

The link ID is a number that the ComProbe software assigns to identify a pair of devices in a BR/EDR connection. In the **Frame Display** details pane, the Baseband layer contains the link ID field if the field's value is not 0.

An Access Address is contained in every *Bluetooth* low energy packet. The Access Address identifies a connection between a slave and a master or an advertising packet.

Connection filtering displays only the frames, protocols, summary, details, and events for the selected connections.

Note: Connection Filters are not persistent across sessions.

4.4.1.13.2.1 Creating a Connection Filter

In the Frame Display there are four ways to create a connection filter.

From the Frame Display Filter menu

Click on the **Frame Display Filter** menu **Connection Filter** selection. From the drop down menu, select **Classic** or **Bluetooth low energy**. The options are

- Classic *Bluetooth*:
  - **All** will filter in all Classic *Bluetooth* frames. You are in effect filtering out any *Bluetooth* low energy frames and are selecting to filter in all the Classic *Bluetooth* links.
  - **Links** displays all the master-slave links. You can select only one link to filter in. The selected link will filter in only the frames associated with that link.
- *Bluetooth* low energy:
  - **All** will filter in all Bluetooth low energy frames. You are in effect filtering out any Classic Bluetooth frames and are selecting to filter in all Bluetooth low energy access addresses.
  - **Access Addresses** displays all the low energy slave device's access address. You can select only one access address to filter. The selected link will filter in only the frames associated with that access address.
- 802.11:
  - **All** will filter in all 802.11 frames. You are in effect filtering out any other technology frames.
- HCI:
  - **All** will filter in all HCI frames. You are in effect filtering out any other technology frames.

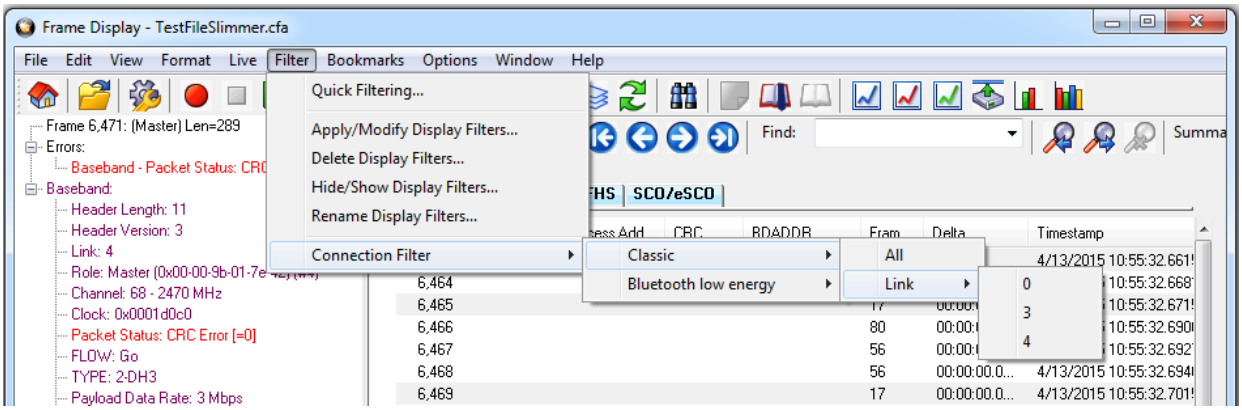


Figure 4.37 - Connection Filter from the Frame Display Menu

From the Frame Display toolbar

Right-click anywhere in the toolbar and select **Connection Filter** from the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

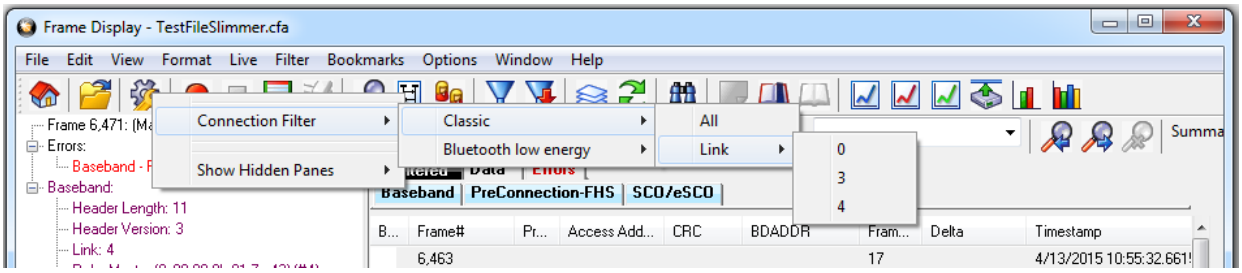


Figure 4.38 - Connection Filter from the Frame Display Toolbar right-click

From the Frame Display panes

Right-click anywhere in a Frame Display pane and select **Connection Filter** in the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

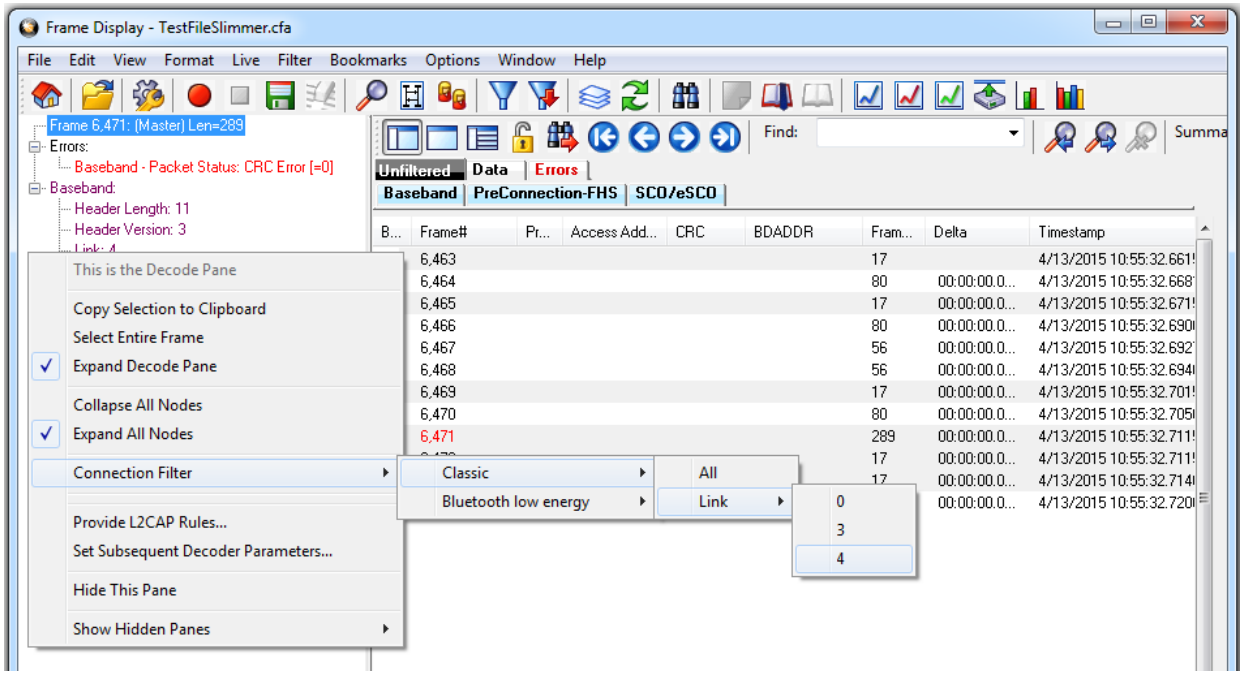


Figure 4.39 - Connection Filter from the Frame Display Pane right-click

From the Frame Display frame selection

Select a frame in the summary pane. Right-click and select **Connection Filter** in the pop-up menu. The procedure for creating a connection filter are identical as described in **From the Frame Display Filter menu**, above.

If the frame you have selected is associated with a Classic *Bluetooth* link or a *Bluetooth* low energy access address, an additional pop-up menu item will appear as shown in the example image below. This selection is a predetermined filter based on your selection. In the example, frame "6471" is associated with "Link 4", so the predetermined filter assumes that you may want create a connection filter for that link. Clicking on **Connection Filter Link = 4** will filter in "Link 4" frames without opening all the drop-down menus.

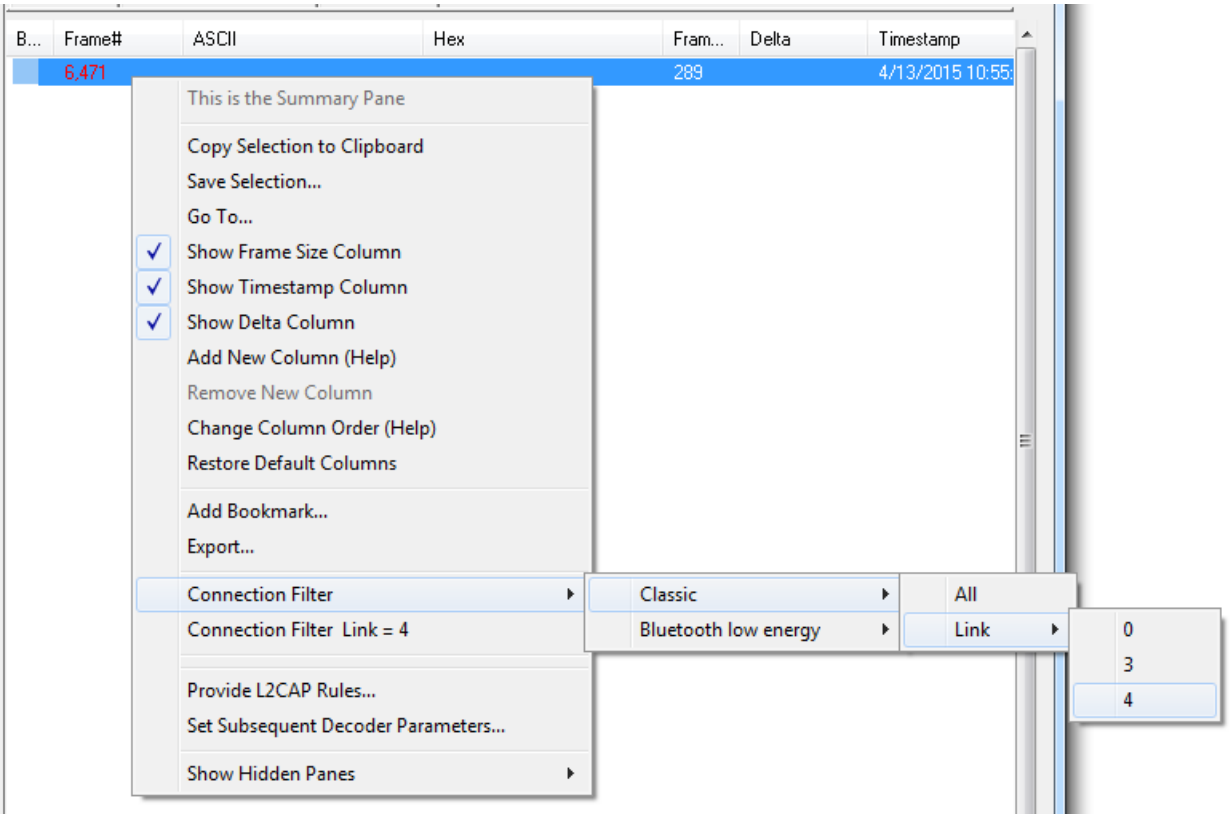


Figure 4.40 - Connection Filter from frame selection right-click

Creating from any Frame Display window

A Connection Filter can be created from any open Frame Display window, and the filtering will always be applied to the original captured data set.

4.4.1.13.2.2 Connection Filter Display

Once you have selected which connections to filter in, another Frame Display will open. The original Frame Display will remain open, and can be minimized.

Note: The system currently limits the number of frame displays to 5. This limit includes any Frame Displays opened using Duplicate View from the Toolbar (see Working with Multiple Frame Displays on page 70)

The new Frame Display with the filtered connection frames will only contain the data defined by the filter criteria. That is, the criteria could be a single link or data for a particular technology.

Display Example 1: Bluetooth low energy Access Address selected

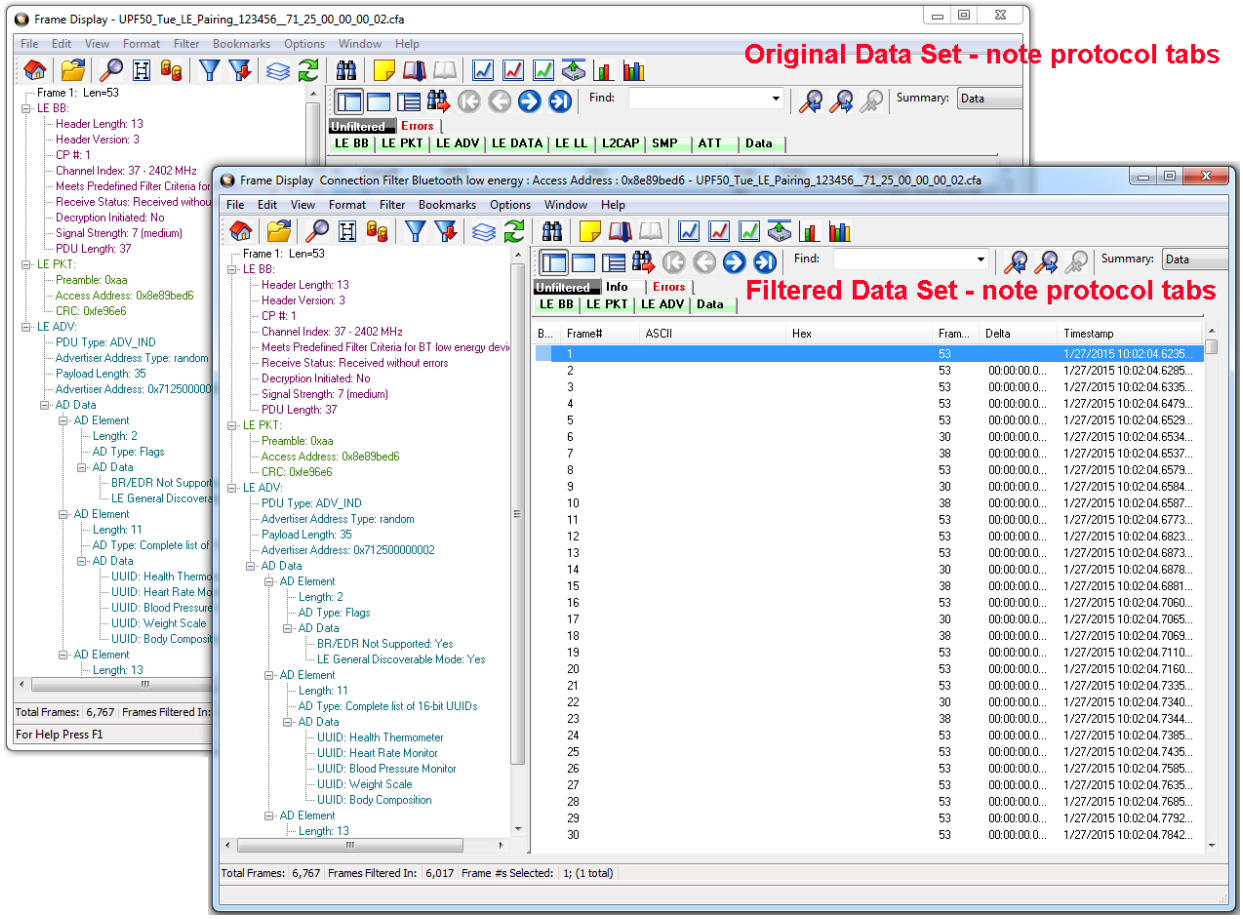


Figure 4.41 - Front Display: Filtered on Access Address 0x8e89bed6

In the figure above is an example Bluetooth low energy data set connection filtered on Access Address = 0x8e89bed6. The Frame Display in the front is the filtered data set. One way to note the difference between the original and the filtered display is to observe the Protocol Tabs. In the filtered display there are four low energy protocol tabs as compared to nine in the original display. This access address connection is not using five of the protocols.

From any open Frame display the user can set another Connection Filter based on the original data set.

Display Example 2: All 802.11 data filtered in

In this example, there is a capture file with Classic *Bluetooth*, *Bluetooth* low energy, and 802.11. To view just the 802.11 data set, 802.11 = All is selected from the right-click pop up menu.

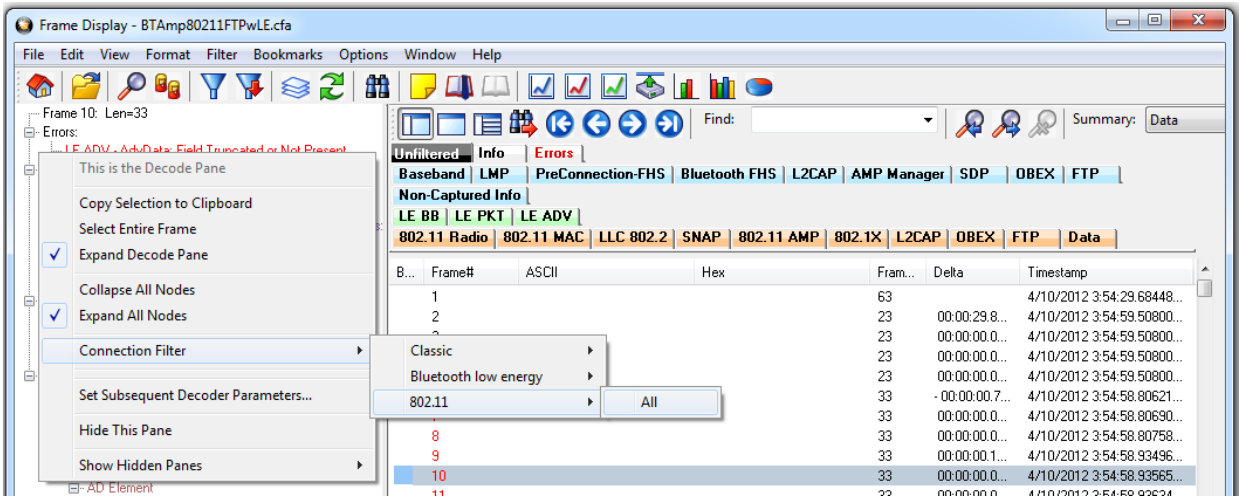


Figure 4.42 - Unfiltered: Capture File with Classic, low energy, and 802.11

When the Frame Display with the filtered 802.11 data set appears, only the Protocol Tabs for 802.11 are present and the tabs for Classic *Bluetooth* and *Bluetooth* low energy have been filtered out.

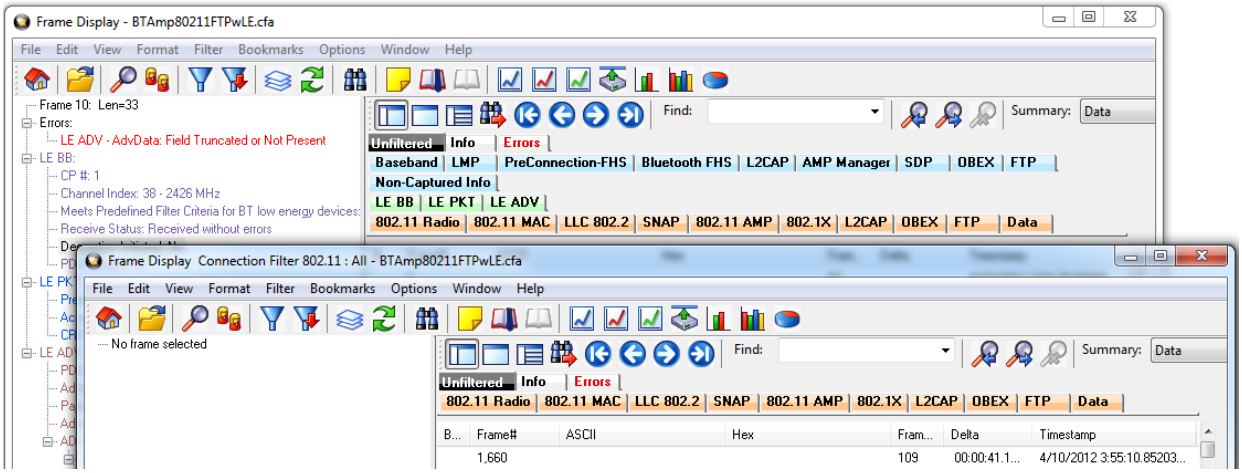

Frame Display - BTAmp80211FTPwLE.cfa
Frame Display Connection Filter 802.11 : All - BTAmp80211FTPwLE.cfa
No frame selected
Find:
Summary:
Data
Unfiltered Info Errors
802.11 Radio 802.11 MAC LLC 802.2 SNAP 802.11 AMP 802.1X L2CAP OBEX FTP Data
B... Frame# ASCII Hex Fram... Delta Timestamp

Figure 4.43 - Connection Filter selecting All 802.11 frames, front

4.4.1.13.3 Protocol Filtering from the Frame Display

4.4.1.13.3.1 Quick Filtering on a Protocol Layer

On the **Frame Display** , click the **Quick Filtering** icon or select **Quick Filtering** from the **Filter** menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

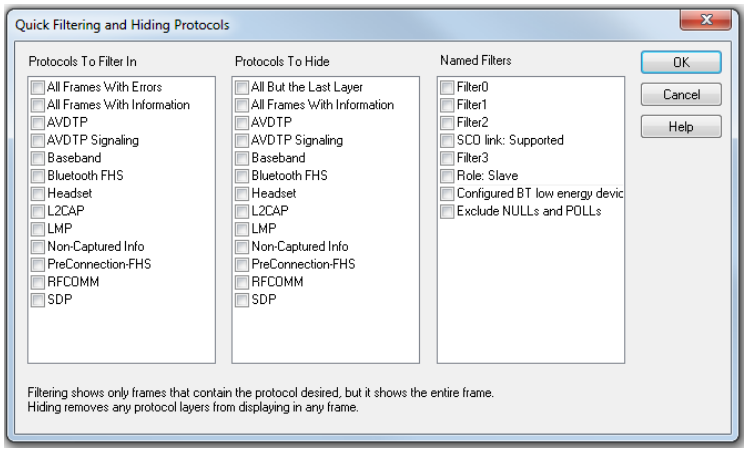


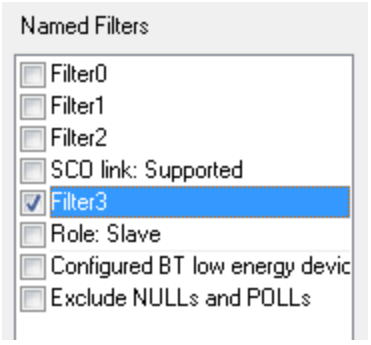
Figure 4.44 - Frame Display Quick Filtering and Hiding Protocols Dialog

The box on the left is **Protocols To Filter In**. When you select the checkbox for a protocol in the **Protocols to Filter In**, the **Summary** pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A **Quick Filter** tab then appears on the **Frame Display**. Changing the filter definition on the **Quick Filter** dialog changes the filter applied on the **Quick Filter** tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**. When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the **Decode**, **Binary**, **Radix**, and **Character** panes. The frames containing that type data will still appear in the **Summary** pane, but not in the **Decode**, **Binary**, **Radix**, and **Character** panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs. When you select the checkbox for the **Name Filters**, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.



Check the small box next to the name of each protocol you want to filter in, hide, or **Named Filter** to display.

Then click **OK**

4.4.1.13.3.2 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the **Summary** pane, and the second lets you filter on any protocol discovered on the network so far.

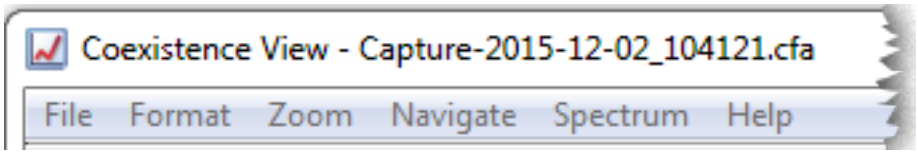
4.4.2 Coexistence View

The **Coexistence View** displays Classic *Bluetooth*, *Bluetooth* low energy, and 802.11 packets and throughput in one view. You access the **Coexistence View** by clicking its button in the **Control** window or **Frame Display** toolbars, or **Coexistence View** from the **View** menus.

Coexistence View - bpa - (bt+le+wf) (hs) (18,842 packets).cfa
File Format Zoom Navigate Spectrum Help
Packets: All Selected Viewport
Show Zoom
Throughput Over Time
Viewport Packet Range (590 Packets)
Selected Packet: None
2.4 Ghz Channels
Click on any bold entry above to enable navigation
For Help Press F1

Figure 4.45 - Coexistence View Window

4.4.2.1 Coexistence View Menus



The following tables describe each of the Coexistence View Menus.

Table 4.6 - Coexistence View File Menu Selections

Selection	Description
Reset	Resets the Coexistence View window to its default settings.
Exit	Closes the Coexistence View window.

Table 4.7 - Coexistence View Format Menu Selections

Selection	Description
Show Packet Number	When checked, the packet number shows below the packet in the Viewport.

Table 4.7 - Coexistence View Format Menu Selections (continued)

Selection	Description
Show Packet Type	When checked, the packet type shows below the packet in the Viewport.
Show Packet Subtype	When checked, the packet subtype shows below the packet in the Viewport, if applicable.
Hide Packet Text	When checked, hides any text shown below the packet in the Viewport. Applies the text shown by the Show Packet Number, **Show Packet Type**, and **Show Packet Subtype** menu selections.
Auto Hide Packet Text When Duration > 31.25 ms.	When checked, automatically hides any text shown below the packet in the Viewport when the Viewport duration exceeds 31.25 ms. Applies the text shown by the Show Packet Number, **Show Packet Type**, and **Show Packet Subtype** menu selections. The Viewport duration is shown at the bottom of the Viewport. This selection reduces display clutter when viewing a larger timeline section.
Increase Auto Hide Packet Count from 4,000 to 20,000 (May Be Slow)	When not checked, the default, the packets in the viewport are hidden if the number of visible packets exceeds 4,000. When checked, the default count increased from 4,000 to 20,000 packets before the packets are hidden. Choosing this selection may slow down the displaying of the packets.
The following three selections are mutually exclusive.	
Use All Packets for Throughput Indicators	When checked, all captured packets are used for average throughput calculations and all packets in the last one second of the capture session are used for the 1 sec throughput. See Coexistence View - Throughput Indicators on page 105 for more information. Performs the same function as the throughput indicator **All** radio button.
Use Selected Packets for Throughput Indicators	When checked, the packets selected in the Viewport are used for average throughput calculations, and selected packets in the one second before the last selected packet are used for the 1 sec throughput. See Coexistence View - Throughput Indicators on page 105 for more information. Performs the same function as the throughput indicator **Selected** radio button.
Use Viewport Packets for Throughput Indicators	When checked, all packets appearing in the Viewport are used for average throughput calculations, and all packets in the one second before the last packet in the Viewport are used for the 1 sec throughput. See Coexistence View - Throughput Indicators on page 105 for more information. Performs the same function as the throughput indicator **Viewport** radio button.
Set 802.11 Tx Address	When checked, this selection is used to specify the 802.11 source address, where any packet with that source address is considered a Tx packet and is shown with a purple border in the timelines. Performs the same function as the SET button. Refer to Coexistence View - Set Button on page 116
The following three selections are mutually exclusive.	

Table 4.7 - Coexistence View Format Menu Selections (continued)

Selection	Description
Show Packet Throughput	When checked, the Throughput Graph and Throughput Indicator shows data based on packet throughput. Performs the same function as the **Throughput Packet** radio button.
Show Payload Throughput	When checked, the Throughput Graph and Throughput Indicator shows data based on payload throughput. Performs the same function as the **Throughput Payload** radio button.
Show Both Packet And Payload Throughput	When checked, the Throughput Graph will graph both the data based on packets throughput in darker colors and payloay throughput in lighter colors. The Throughput Indicator will show calculations based on packet throughput. Performs the same function as the **Throughput Both** radio button.
The following four selections are mutually exclusive.	
Show 5 GHz Timeline	When checked, the 5 GHz Timeline is visible and the 2.4 GHz Timeline is not visible. Only 802.11 5 GHz packets are shown. Performs the same function as the **Timeline 5 GHz** radio button.
Show 2.4 GHz Timeline	When checked, the 2.4 GHz Timeline is visible and the 5 GHz Timeline is not visible. The timeline will show Classic Bluetooth, Bluetooth Low Energy, and 802.11 2.4 GHz packets. Performs the same function as the **Timeline 2.4 GHz** radio button.
Show Both 2.4 GHz and 5 GHZ Timelines	When checked, the 2.4 GHz Timeline and the 5GHZ Timeline is visible. Performs the same function as the **Timeline Both** radio button.
Show Timelines Which Have or Had Packets (Auto Mode)	When check,shows only timelines which have had packets at some point during this session. If no packets are present, the 2.4 GHz Timeline is visible. Performs the same function as the **Timeline Auto** radio button.
The following two selections are mutually exclusive.	
Show Low Energy Packets From Configurated Devices Only	When checked, shows in the 2.4 GHz Timeline only packets from *Bluetooth* low enegry devices configured for this session, and uses these packets for throughput calculations. Performs the same function as the **LE Devices Configured** radio button.
Show All Low Energy Packets	When checked, shows in the 2.4 GHz Timeline all Bluetooth low energy packets captured in this session, and uses these packets for throughput calculations. Performs the same function as the **LE Devices All** radio button.

Table 4.7 - Coexistence View Format Menu Selections (continued)

Selection	Description
Large Throughput Graph	When checked, the Throughput Graph appears in the bottom half of the window, swapping position with the timeline. When not checked, the Throughput Graph appears in its default position at the top of the window. Performs the same function as clicking the **Swap** button. See Coexistence View - Throughput Graph on page 108.
Show Dots in Throughput Graph (Dots Reveal Overlapped Data Points)	When checked, displays dots on the Throughput Graph. Dots are different sizes for each technology so that they reveal overlapping data points which otherwise wouldn't be visible. A tooltip can be displayed for each dot. Performs the same function as the **Dots** button. See Coexistence View - Throughput Graph on page 108.
Show Zoomed Throughput Graph	When checked, dispalys a Zoomed Throughput Graph above the Throughput Graph. The Zoomed Throughput Graph shows the details of the throughput in the time range covered by the viewport in the Throughput Graph. Performs the same function as the **Show Zoom** button. When not checked, the Zoomed Throughput Graph is hidden. Performs the same function as the **Hide Zoom** button. See Coexistence View - Throughput Graph on page 108 .
Freeze Y Scales in Zoom Throughput Graph	Only active when the Zoomed Throughput Graph is visible. When checked, it freezes the y-axis scales and makes it possible to compare all time ranges and durations. Performs the same fuction as the **Freeze Y** button, which appears with the Zoomed Throughput Graph. When not checked, the y-axis scales are unfroozen. Performs the same function as the **Unfreeze Y** button, which appears with the Zoomed Throughput Graph. See Coexistence View - Throughput Graph on page 108
Show Tooltips in Upper-Left Corner of Screen	When checked, Timeline and Throughput Graph tooltips will appear in the upper-left corner of your computer sceen. You can relocate the tool tip for convenience or to see the timeline or throughput graph unobstructed while displaying packet information. See Coexistence View – Timelines on page 118.

Table 4.8 - Coexistence View Zoom Menu Selections

Selection	Description	Hot Key
Zoom In	When clicked, Viewport time duration decreased.	Ctrl+Plus

Table 4.8 - Coexistence View Zoom Menu Selections (continued)

Selection	Description	Hot Key
Zoom Out	When clicked, Viewport time duration increases	Ctrl+Minus
The following two selectioins are mutually exclusive.		
Scroll Tool (Mouse Wheel Scrolls - Ctrl Key Switches to Zoom Tool)	When checked, sets the mouse wheel to scroll the Viewport. Pressing the Ctrl key while scrolling switches to zooming the Viewport.	
Zoom Tool (Mouse Wheel Zooms- Ctrl Key Switches to Scroll Tool)	When checked, sets the mouse wheel to zoom the Viewport. Pressing the Ctrl key while zooming switches to scrolling the Viewport.	
Zoom To Time Range of Selected Packets	Active only when packets are selected. When clicked, the Viewport duration changes to the time range covered by the selected packets.	
Zoom To Throughput Graph Data Point	When clicked, the Viewport duration changes to the time range of the Throughput Graph selected data point.	
Custom Zoom (Set by Zoom To Time Range of Selected Packets, Zoom To Throughput Graph Data Point, or dragging Viewport Slide)	Automatically checked when taking any zoom action other than the fixed Viewport zoom durations listed below.	

Table 4.8 - Coexistence View Zoom Menu Selections (continued)

Selection	Description	Hot Key
The following 21 selections are mutually exclusive.		
150 usec	Each of these Zoom selections sets the Viewport and the Timeline to a fixed time duration.	
300 usec		
625 usec (1 Bluetooth slot)		
1.25 msec (2 Bluetooth slots)		
1.875 msec (3 Bluetooth slots)		
2.5 msec (4 Bluetooth slots)		
3.125 msec (5 Bluetooth slots)		
6.25 msec (10 Bluetooth slots)		
15.625 msec (25 Bluetooth slots)		
31.25 msec (30 Bluetooth slots)		
62.5 msec (100 Bluetooth slots)		
156.255 msec (250 Bluetooth slots)		
31.25 msec (500 Bluetooth slots)		
625 msec (1,000 Bluetooth slots)		
1 sec (1,600 Bluetooth slots)		
2 sec (3,200 Bluetooth slots)		
3 sec (4,800 Bluetooth slots)		
4 sec (6,400 Bluetooth slots)		
5 sec (8,000 Bluetooth slots)		
10 sec (16,000 Bluetooth slots)		
20 sec (32,000 Bluetooth slots)		

Note: Right-clicking anywhere in the **Coexistence View** window will open the **Zoom** menu in a pop-up.

Table 4.9 - Coexistence View Navigate Menu Selections

Selection	Description	Hot key
First Packet	When clicked, the first packet in the session is selected and displayed in the Timeline. Performs the same function as the First Packet button.	Home

Table 4.9 - Coexistence View Navigate Menu Selections (continued)

Selection	Description	Hot key
Last Packet	When clicked, the last packet in the session is selected and displayed in the Timeline. Performs the same function as the Last Packet button.	End
Previous Packet	When clicked, the first packet occurring in time prior to the currently selected packet is selected and displayed in the Timeline. Performs the same function as the Previous Packet button.	Left Arrow
Next Packet	When clicked, the first packet occurring next in time from the currently selected packet is selected and displayed in the Timeline. Performs the same function as the Next Packet button.	Right Arrow
Previous Retransmitted Packet	When clicked, selects the first prior retransmitted packet from the current selection and displays it in the Timeline.. Performs the same function as the Previous Retransmitted Packet button.	
Next Retransmitted Packet	When clicked, selects the next retransmitted packet from the current selection and displays it in the Timeline.. Performs the same function as the Next Retransmitted Packet.	
Previous Invalid IFS Packet	When clicked, selects the first prior invalid *Bluetooth* low energy IFS packet from the current selection and displays it in the Timeline. Performs the same function as the Previous Invalid IFS Packet button.	
Next Invalid IFS Packet	When clicked, selects the next invalid *Bluetooth* low energy IFS packet from the current selection and displays it in the Timeline. Performs the same function as the Next Invalid IFS Packet button.	
Previous Error Packet	When clicked, selects the first prior packet with an error from the current selection and displays it in the Timeline. Performs the same function as the Previous Error Packet button.	Ctrl+Left Arrow
Next Error Packet	When clicked, selects the next packet with an error from the current selection and displays it in the Timeline. Performs the same function as the Next Error Packet button.	Ctrl+Right Arrow

Table 4.9 - Coexistence View Navigate Menu Selections (continued)

Selection	Description	Hot key
First Legend Packet	When clicked, selects the first legend packet in the session and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to Coexistence View – Legend on page 118. Performs the same functions as the First Legend Packet button.	
Previous Legend Packet	When clicked, selects the first prior legend packet in time from the current selection and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to Coexistence View – Legend on page 118. Performs the same functions as the Previous Legend Packet button.	
Next Legend Packet	When clicked, selects the next legend packet in time from the current selection and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to Coexistence View – Legend on page 118. Performs the same functions as the Next Legend Packet button.	
Last Legend Packet	When clicked, selects the last legend packet in the session and displays it in the Timeline. This control is enabled when a bold packet type is selected in the Coexistence View Legend. Refer to Coexistence View – Legend on page 118. Performs the same functions as the Last Legend Packet button.	
Toggle Display Lock	This selection is active during Live capture mode only. Checking this selection will lock the Throughput Graph and the Timeline in its current position, however the capture will continue. Not checking this selection will cause the Throughput Graph and the Timeline to scroll as data is collected.	

Note: Navigate menu selections are context sensitive. For example, If the first packet is selected, the **Next Packet** and the **Last Packet** selections are active, but the **Previous Packet** selection is inactive.

4.4.2.2 Coexistence View - Toolbar

Figure 4.46 - Coexistence View Toolbar

The toolbar contains the following selections:

Table 4.10 - Coexistence View Toolbar icons

Icon	Description
	Move to the first packet.
	Move to the previous packet.

Table 4.10 - Coexistence View Toolbar icons (continued)

Icon	Description
	Move to the next packet.
	Move to the last packet.
	Move to the previous retransmitted packet.
	Move to the next retransmitted packet
	Move to the previous invalid IFS for *Bluetooth* low energy.
	Move to the next invalid IFS for *Bluetooth* low energy.
	Move to the previous bad packet.
	Move to the next bad packet.
	Move to the first packet of the type selected in the legend.
	Move to the previous packet of the type selected in the legend
	Move to the next packet of the type selected in the legend.
	Move to the last packet of the type selected in the legend.
	Zoom in.
	Zoom out.
	Scroll cursor.
	When selected the cursor changes from Scroll to a context-aware zooming cursor. Click on normal cursor to remove the zooming cursor.
	Zooming cursor.

Table 4.10 - Coexistence View Toolbar icons (continued)

Icon	Description
	Scroll Lock/Unlock during live capture mode.
	Reset during live capture mode. Clears the display.

4.4.2.3 Coexistence View - Throughput Indicators

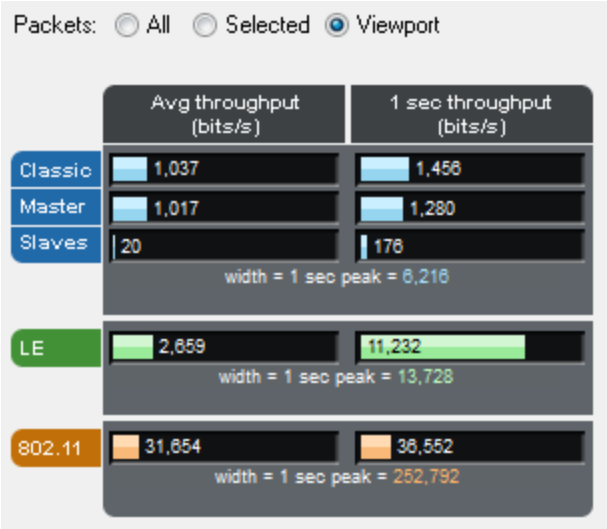


Figure 4.47 - Coexistence View Throughput Indicators

Throughput indicatorsshow average throughput and 1 second throughput for Classic Bluetooth® (all devices, master devices, and slave devices are each shown separately), *Bluetooth* low energy, and 802.11.

4.4.2.4 Throughput

Throughput is total packet or payload size in bits of the included packets divided by the duration of the included packets, where:

- *Packet size* is used if the Packet or Both radio button is selected in the Throughput group.
- *Payload size* is used if the Payload radio button is selected in the Throughput group.
- *Included packets* are defined separately for each of the radio buttons that appear above the throughput indicators.
- *Duration of the included packets* is measured from the beginning of the first included packet to the end of the last included packet.

4.4.2.5 Radio Buttons

The radio buttons above the throughput indicators specify which packets are *included*. Radio button descriptions are modified per the following:

- *Bluetooth* low energy packets from non-configured devices are excluded if the **Configured** radio button in the LE Devices group is selected.
- **Frame Display** filtering has no effect here in that packets that are filtered-out in **Frame Display** are still used here as long as they otherwise meet the criteria for each radio button as described below.

4.4.2.6 All radio button

All packets are used for average throughput, and packets occurring in the last 1 second of the session are used for 1 second throughput, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

4.4.2.7 Selected radio button

Selected packets (the selected packet range is shown in the timeline header) are used for average throughput, and packets in the 1 second duration ending at the end of the last selected packet are used for 1 second, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

Figure 4.11 Timeline Header Showing Selected Packets

4.4.2.8 Viewport radio button

The viewport is the purple rectangle in the **Throughput Graph** and indicates a specific starting time, ending time, and resulting duration. Packets that occur within that range of time are used for average throughput, and packets in the 1 second duration ending at the end of the last packet in the viewport time range are used for 1 second throughput, except that *Bluetooth* low energy packets from non-configured devices can be excluded as noted above.

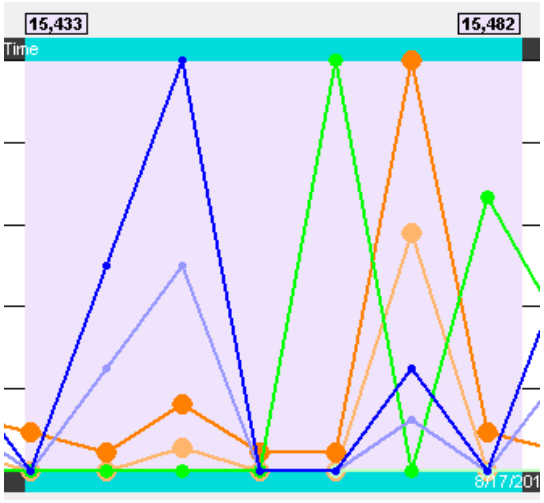


Figure 4.48 - **Throughput Graph** viewport.

4.4.2.9 Indicator width

The width of each indicator is the largest 1 second throughput seen up to that point for that technology (Classic *Bluetooth*, *Bluetooth* low energy, or 802.11), where the 1 second throughput is calculated anew each time another packet is received. The 1 second throughput indicator will never exceed this width, but the average throughput indicator can. For example, the image below has a large average throughput because the Selected radio button was selected and a single packet was selected, and the duration in that case is the duration of the single packet, which makes for a very small denominator in the throughput calculation. When the average throughput exceeds the indicator width, a plus sign (+) is drawn at the right end of the indicator.

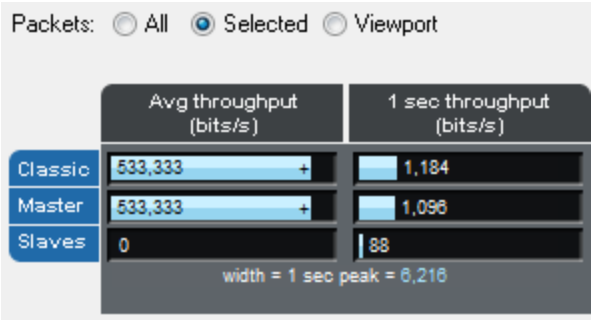


Figure 4.49 - Average throughput indicators show a plus sign (+) when the indicator width is exceeded.

Figure 4.50 - A single selected packet

4.4.2.10 Coexistence View - Throughput Graph

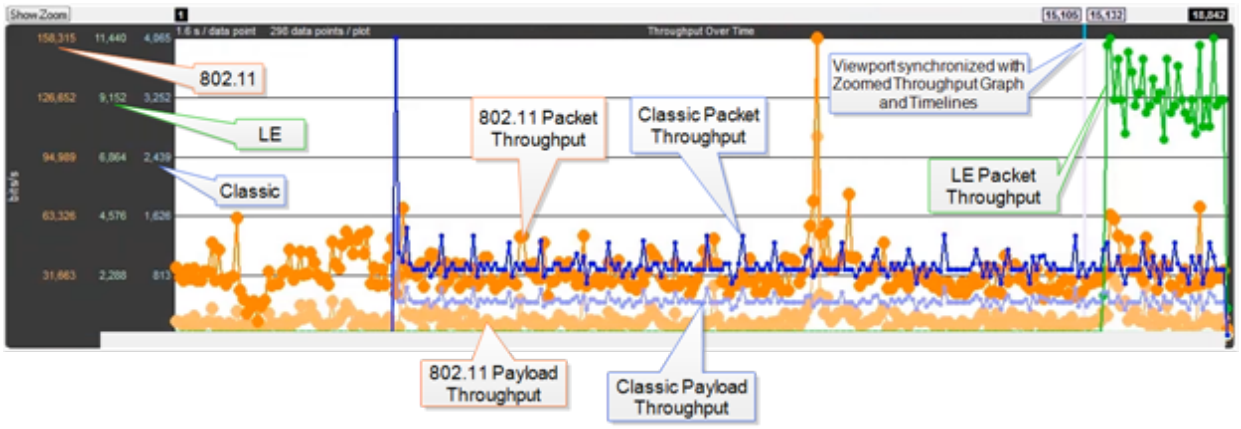


Figure 4.51 - Coexistence View Throughput Graph

The **Throughput Graph** is a line graph that shows packet and/or payload throughput over time as specified by the radio buttons in the Throughput group. If the **Both** radio button is selected, packet and payload throughput are shown as two separate lines for each technology. The payload throughput line is always below the packet throughput line (unless both are 0).

The data lines and y-axis labels are color-coded: Blue = Classic Bluetooth® , Green = *Bluetooth* low energy, Orange = 802.11. Each data point represents a duration which is initially 0.1 s. Each time the number of data points per line reaches 300, the number of data points per line is halved to 150 and the duration per data point is doubled. The duration per data point thus progresses from 0.1 s to 0.2 s to 0.4 s to 0.8 s and so on.

4.4.2.11 Throughput Graph Y-axis labels

The y-axis labels show the throughput in bits per second. From left-to-right the labels are for 802.11, *Bluetooth* low energy, and Classic *Bluetooth*. The duration of each data point must be taken into account for the y-axis label's value to be meaningful. For example, if a data point has a duration of 0.1 s and a bit count of 100, it will have a throughput of 1,000 bits/s, and the y-axis labels will be consistent with this.

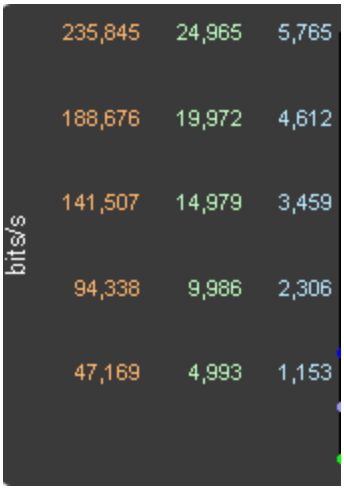


Figure 4.52 - **Throughput Graph** y-axis labels.

4.4.2.12 Excluded packets

Retransmitted packets and bad packets (packets with CRC or Header errors) are excluded from throughput calculations.

4.4.2.13 Tooltips

Placing the mouse pointer on a data point shows a tooltip for that data point. The tooltip first line shows the throughput, the throughput type (packet or payload), and the technology. Subsequent lines show the bit count, the duration of the data point, the packet range of that duration (only packets of the applicable technology from that packet range are used for the throughput calculation), and the number of the data point (which is 0 for the first data point in each line).

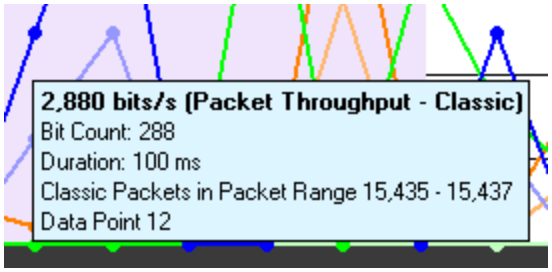

2,880 bits/s (Packet Throughput - Classic)
Bit Count: 288
Duration: 100 ms
Classic Packets in Packet Range 15,435 - 15,437
Data Point 12

Figure 4.53 - Data point tooltip

The Throughput graph tool tips can be shown in the upper-left corner of your computer screen to provide an unobstructed view. Refer to Relocating Tool Tips.

4.4.2.14 Discontinuities

A discontinuity is when the timestamp going from one packet to the next either goes backward by any amount or forward by more than 4.01 s. This value is used because the largest possible connection interval in *Bluetooth* low energy is 4.0 s. A discontinuity is drawn as a vertical dashed line. A discontinuity for a

timestamp going backward is called a negative discontinuity and is shown in red. A discontinuity for a timestamp going forward by more than 4.01 s is called a positive discontinuity and is shown in black. A positive discontinuity is a cosmetic nicety to avoid lots of empty space. A negative discontinuity is an error.

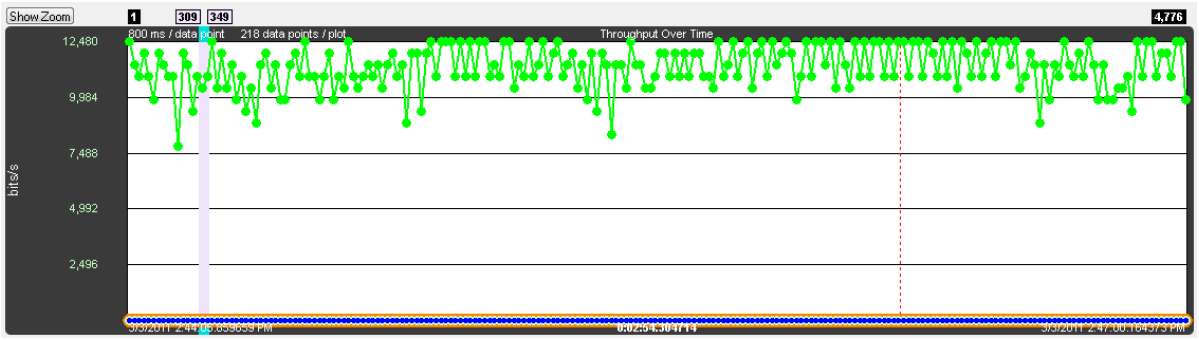


Figure 4.54 - A negative discontinuity.

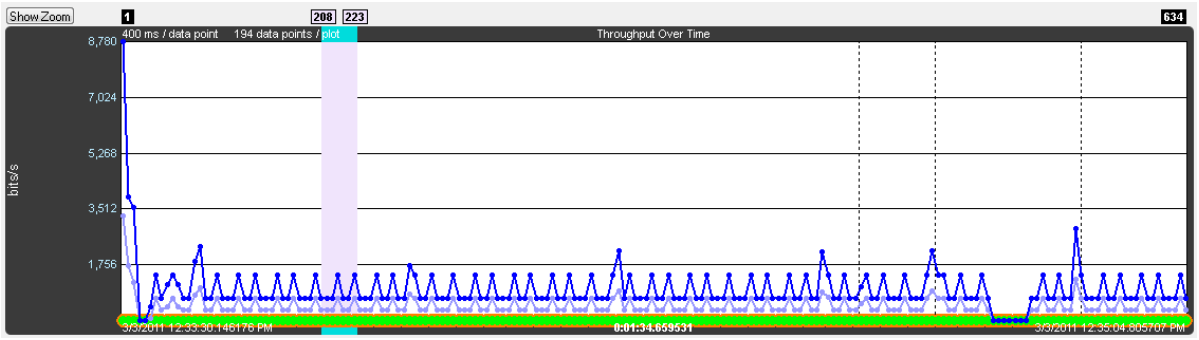


Figure 4.55 - Three positive discontinuities.

4.4.2.15 Viewport

The viewport is the purple rectangle in the **Throughput Graph**. It indicates a specific starting time, ending time, and resulting duration, and is precisely the time range used by the **Timeline**. The packet range that occurs within this time range is shown above the sides of the viewport.

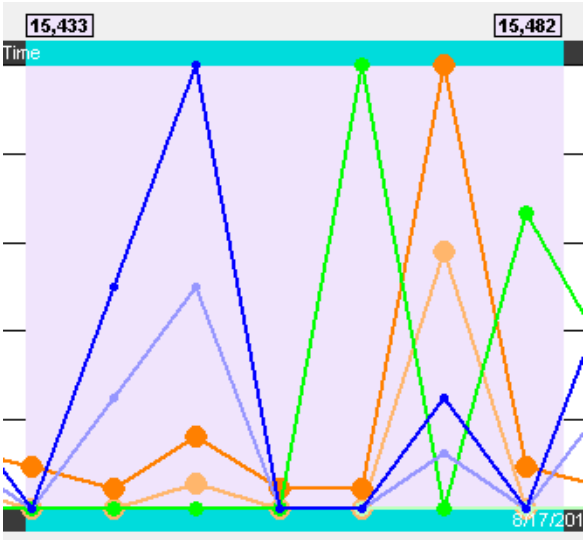


Figure 4.56 - **Throughput Graph** Viewport

The viewport is moved by dragging it or by clicking on the desired location in the **Throughput Graph** (the viewport will be centered at the click point).

The viewport is sized by dragging one of its sides or by using one of the other zooming techniques. See the Zooming subsection in the **Timeline** section for a complete list.

4.4.2.16 Swap button

The **Throughput Graph** and **Timeline** can be made to trade positions by clicking the **Swap** button.

Clicking the Swap

button swaps the positions of the **Throughput Graph**s and the **Timeline**s.

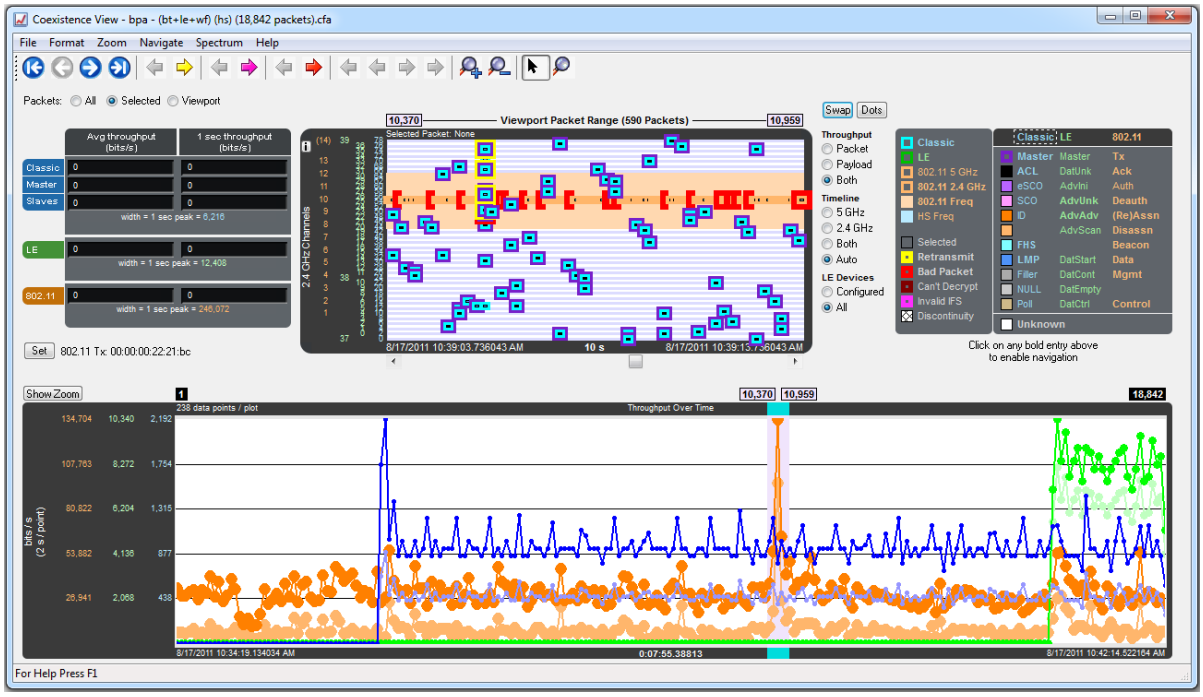


Figure 4.57 - Small Timeline and large Throughput Graph after pressing the Swap button.

4.4.2.17 Dots button

The dots on the data points can be toggled on and off by clicking the **Dots**

button. Dots are different sizes for each technology so that they reveal overlapping data points which otherwise wouldn't be visible. A tooltip can be displayed for each dot.

Dots can be removed for greater visibility of the plots when data points are crowded together.

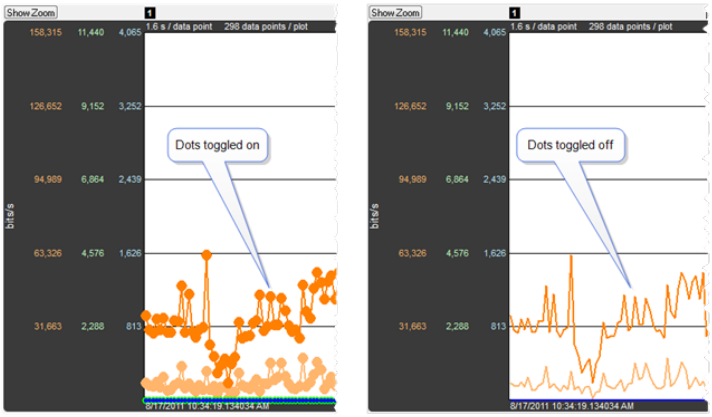


Figure 4.58 - Dots Toggled On and Off

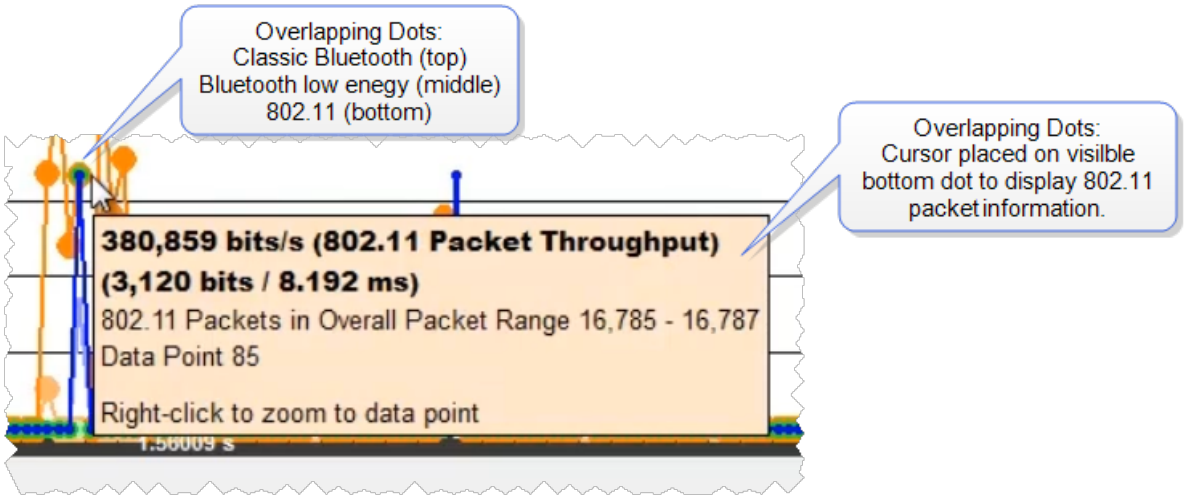

Overlapping Dots:
Classic Bluetooth (top)
Bluetooth low enegy (middle)
802.11 (bottom)
Overlapping Dots:
Cursor placed on visilble
bottom dot to display 802.11
packet information.
380,859 bits/s (802.11 Packet Throughput)
(3,120 bits / 8.192 ms)
802.11 Packets in Overall Packet Range 16,785 - 16,787
Data Point 85
Right-click to zoom to data point

Figure 4.59 - Overlapping **Dots** Information Display

4.4.2.18 Zoomed Throughput Graph

Clicking the **Show Zoom** button Show Zoom displays the **Zoomed Throughput Graph** above the **Throughput Graph**. The **Zoomed Throughput Graph** shows the details of the throughput in the time range covered by the viewport in the **Throughput Graph**. Both the **Zoomed Throughput Graph** and the **Timelines** are synchronized with the **Throughput Graph**'s viewport. The viewport is sized by dragging one of its sides or by using one of the other zooming techniques listed in the Zooming subsection in the **Timelines** section.

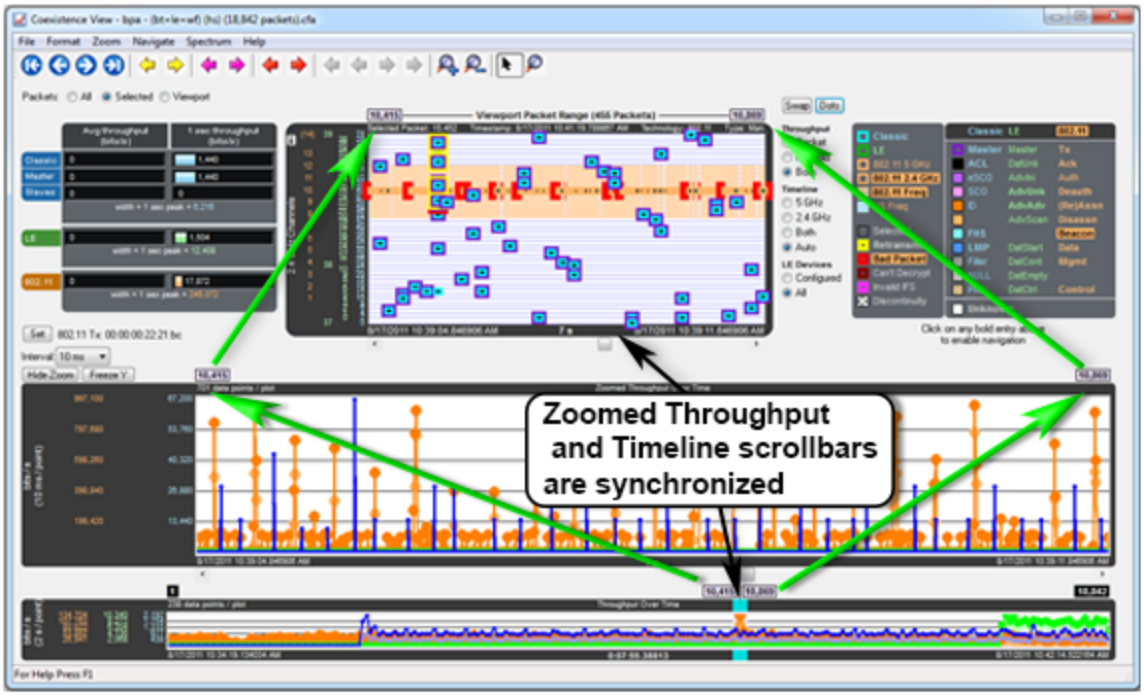


Figure 4.60 - Synchronized Zoomed Throughput Graph and View Port

The largest value in each technology in the **Zoomed Throughput Graph** is snapped to the top of the graph. This makes the graph easier to read by using all of the available space, but because the y-axis scales can change it can make it difficult to compare different time ranges or durations. Clicking the **Freeze Y** Freeze Y button freezes the y-axis scales and makes it possible to compare all time ranges and durations (the name of the button changes to **Unfreeze Y** and a **Y Scales Frozen** indicator appears to the right of the title. Clicking the **Unfreeze Y** Unfreeze Y button unfreezes the y-axis scales.

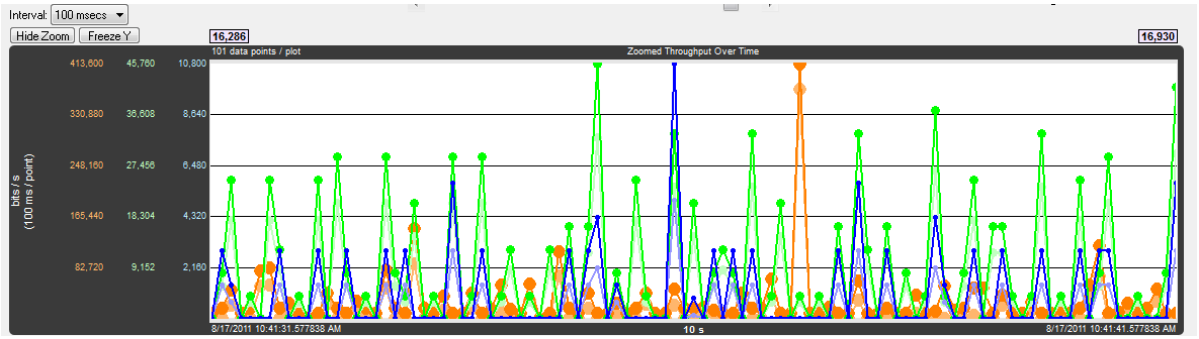


Figure 4.61 - **Zoomed Throughput Graph**- Largest Value Snaps to Top

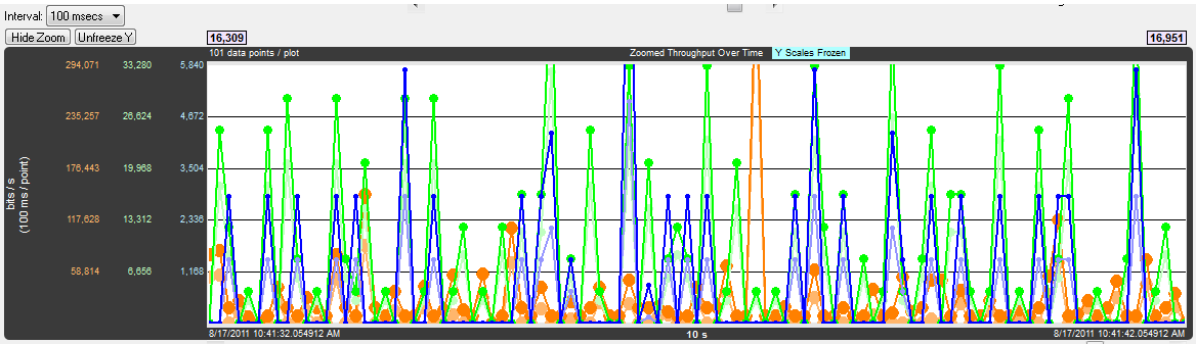
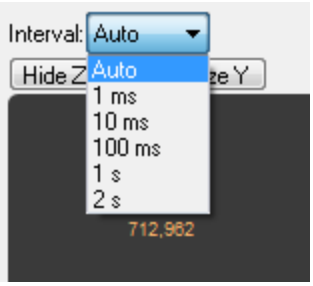


Figure 4.62 - **Zoomed Throughput Graph** - **Freeze Y** keeps the y-axis constant

Interval Menu



The **Interval** drop-down menu is used to set the duration of each data point in the Zoomed Throughput graph. The default setting is **Auto** that sets the data point interval automatically depending on the zoom level. The other menu selections provide the ability to select a fixed data point interval. Selecting from a larger to a smaller interval will display more data points. Should the number of data points exceed 30,000, no data is displayed and a warning will appear in the graph area.

4.4.2.19 Zoom Cursor

Selecting the **Zoom Cursor** button changes the cursor to the zoom cursor. The zoom cursor is controlled by the mouse wheel and zooms the viewport and thus the Timelines and the Zoomed Throughput Graph. The zoom cursor appears everywhere except the **Throughput Graph**, which is not zoomable, in which case the scroll cursor is shown. When the zoom cursor is in the **Timelines** or **Zoomed Throughput Graph** zooming occurs around the point in time where the zoom cursor is positioned. When the zoom cursor is outside the **Timelines** and the **Zoomed Throughput Graph** the left edge of those displays is the zoom point.

4.4.2.20 Comparison with the *Bluetooth* Timeline's Throughput Graph

The **Throughput Graph**s for Classic *Bluetooth* in the **Coexistence View** and the *Bluetooth***Timeline** can look quite different even though they are plotting the same data. The reason is that the **Coexistence View** uses timestamps while the *Bluetooth***Timeline** uses *Bluetooth* clocks, and they do not always match up exactly. This mismatch can result in the data for a particular packet being included in different intervals in the two **Throughput Graph**s, and can have a significant impact on the shapes of the two respective graphs. This can also result in the total duration of the two **Throughput Graph**s being different.

Another factor that can affect total duration is that the *Bluetooth***Timeline**'s **Throughput Graph** stops at the last Classic *Bluetooth* packet while the **Coexistence View**'s **Throughput Graph** stops at the last packet regardless of technology.

4.4.2.21 Coexistence View - Set Button

The **Set** button is used to specify the 802.11 source address, where any packet with that source address is considered a Tx packet and is shown with a purple border in the timelines.

All source MAC addresses that have been seen during this session are listed in the dialog that appears when the **Set** button is clicked. Also listed is the last source MAC address that was set in the dialog in the previous session. If that address has not yet been seen in this session, it is shown in parentheses.

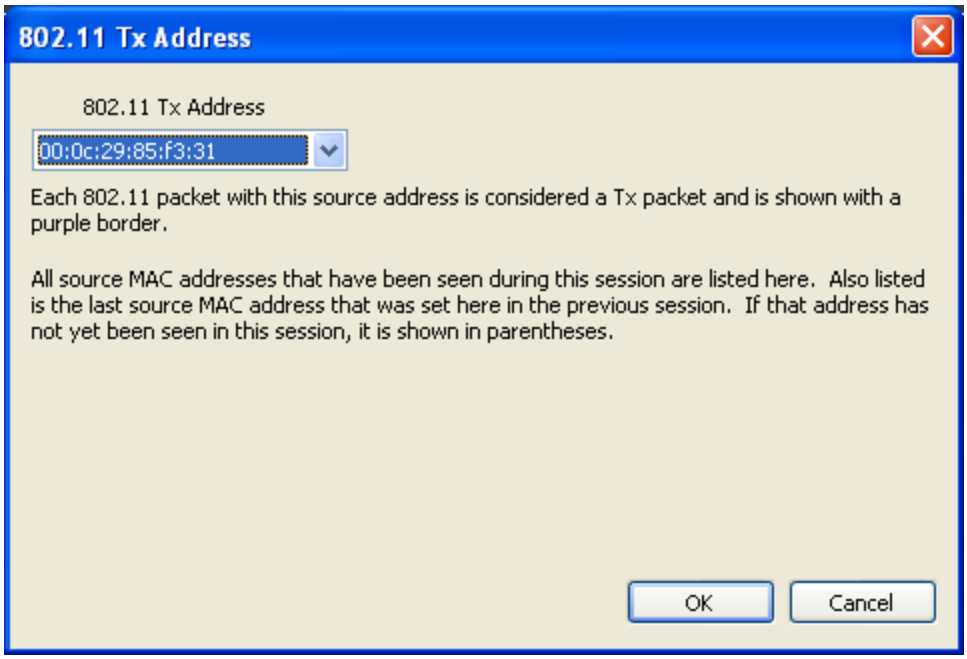

802.11 Tx Address
802.11 Tx Address
00:0c:29:85:f3:31
Each 802.11 packet with this source address is considered a Tx packet and is shown with a purple border.
All source MAC addresses that have been seen during this session are listed here. Also listed is the last source MAC address that was set here in the previous session. If that address has not yet been seen in this session, it is shown in parentheses.
OK
Cancel

Figure 4.63 - 802.11 Source Address Dialog

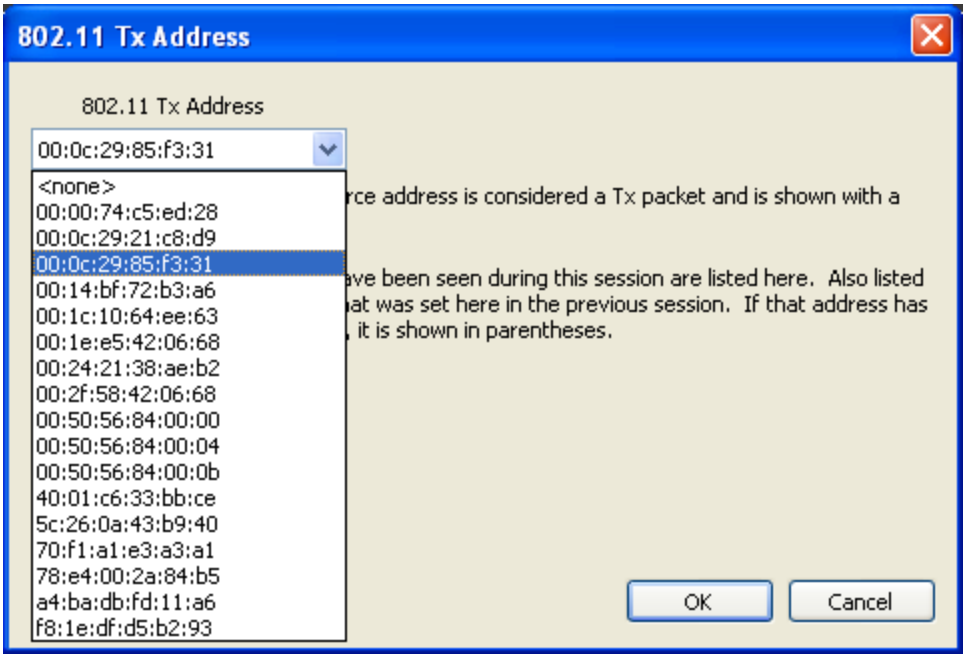
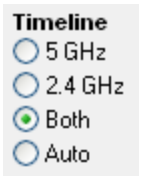


Figure 4.64 - 802.11 Source Address Drop Down Selector

4.4.2.22 Coexistence View - Throughput Radio Buttons

The radio buttons in the Throughput group specify whether to show packet and/or payload lines in the Throughput Graph, and also whether to show packet or payload throughput in the throughput indicators (if the Both radio button is selected, packet throughput is shown in the throughput indicators).

4.4.2.23 Coexistence View - Timeline Radio Buttons



The radio buttons in the **Timeline** group specify timeline visibility. The first three buttons specify whether to show one or both timelines, while the **Auto** button shows only timelines which have had packets at some point during this session. If no packets have been received at all and the **Auto** button is selected the 2.4 GHz timeline is shown.

4.4.2.24 Coexistence View – low energy Devices Radio Buttons

The radio buttons in the **LE Devices** group (where "LE" means Bluetooth® low energy) specify both visibility and inclusion in throughput calculations of *Bluetooth* low energy packets. The **All** radio button shows and uses all *Bluetooth* low energy packets. The Configured radio button shows and uses only *Bluetooth* low energy packets which come from a configured device.

4.4.2.25 Coexistence View – Legend

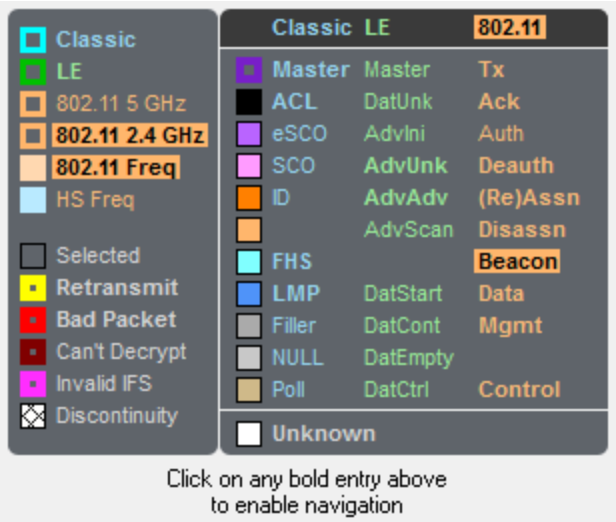


Figure 4.65 - Coexistence View Legend

The legend describes the color-coding used by packets in the timelines. Selecting a packet in a timeline highlights the applicable entries in the legend. An entry is bold if any such packets currently exist. Clicking on a bold entry enables the black legend navigation arrows in the toolbar for that entry.

4.4.2.26 Coexistence View – Timelines

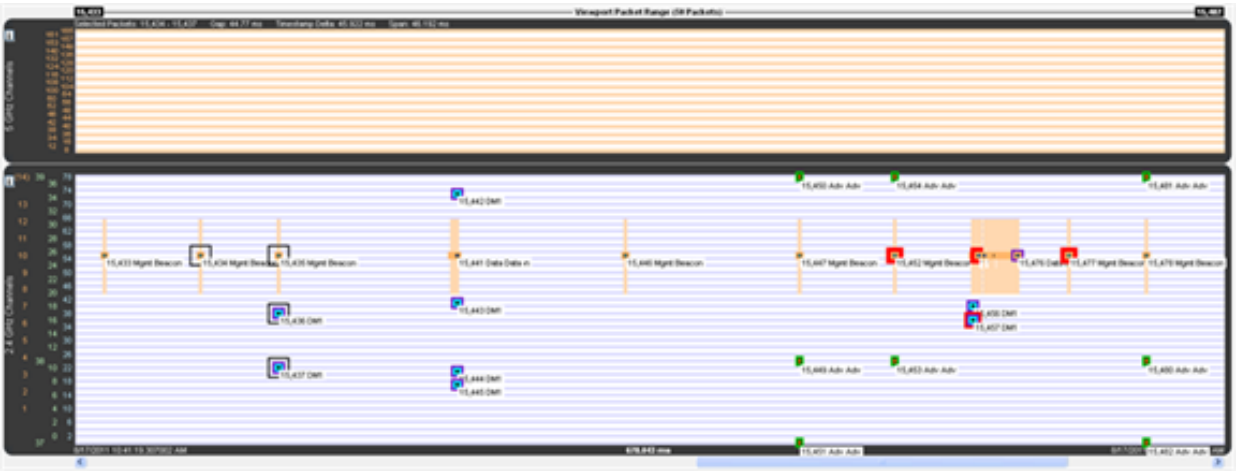


Figure 4.66 - Coexistence View Timelines

The **Timelines** show Classic Bluetooth® , *Bluetooth* low energy, and 802.11 packets by channel and time.

4.4.2.27 Packet information

Packet information is provided in various ways as described below.

Packets are color-coded to indicate attribute (Retransmit, Bad Packet, Can't Decrypt, or Invalid IFS), master/Tx, technology (Classic Bluetooth® , *Bluetooth* low energy, or 802.11), and category/type.

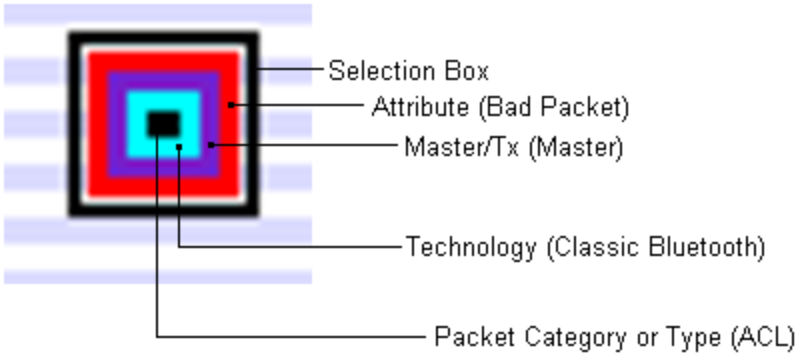


Figure 4.67 - Each packet is color-coded

The innermost box (which indicates packet category/type) is the packet proper in that its vertical position indicates the channel, its length indicates the packet's duration in the air, its left edge indicates the start time, and its right edge indicates the end time.

The height of Classic *Bluetooth* and *Bluetooth* low energy packets indicates their frequency range (1 MHz and 2 MHz respectively). Since 802.11 channels are so wide (22 MHz), 802.11 packets are drawn with an arbitrary 1 MHz height and centered within a separate frequency range box which indicates the actual frequency range.

Selecting a packet by clicking on it draws a selection box around it (as shown above) and highlights the applicable entries in the legend.

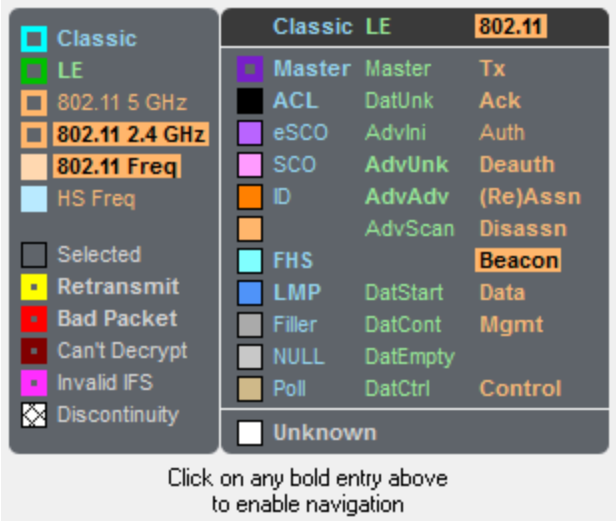


Figure 4.68 - Highlighted entries in the legend for a selected packet.

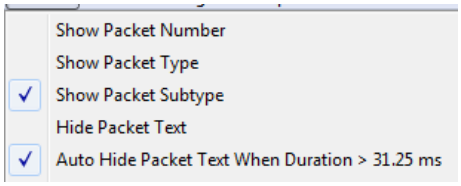
Summary information for a selected packet is displayed in the timeline header.

Selected Packet: 15,457 Timestamp: 8/17/2011 10:41:19.835783 AM Technology: Classic Type: DM1 Bluetooth Clock: 0x0113e610 Payload Len: 9 bytes

Figure 4.69 - **Timeline** header for a single selected packet.

When multiple packets are selected (by dragging the mouse with the left button held down, clicking one packet and shift-clicking another, or clicking one packet and pressing shift-arrow), the header shows **Gap** (duration between the first and last selected packets), **Timestamp Delta** (difference between the timestamps, which are at the beginning of each packet), and **Span** (duration from the beginning of the first selected packet to the end of the last selected packet).

Figure 4.70 - **Timeline** header for multiple selected packets



Text can be displayed at each packet by selecting **Show Packet Number**, **Show Packet Type**, and **Show Packet Subtype** from the **Format** menu.

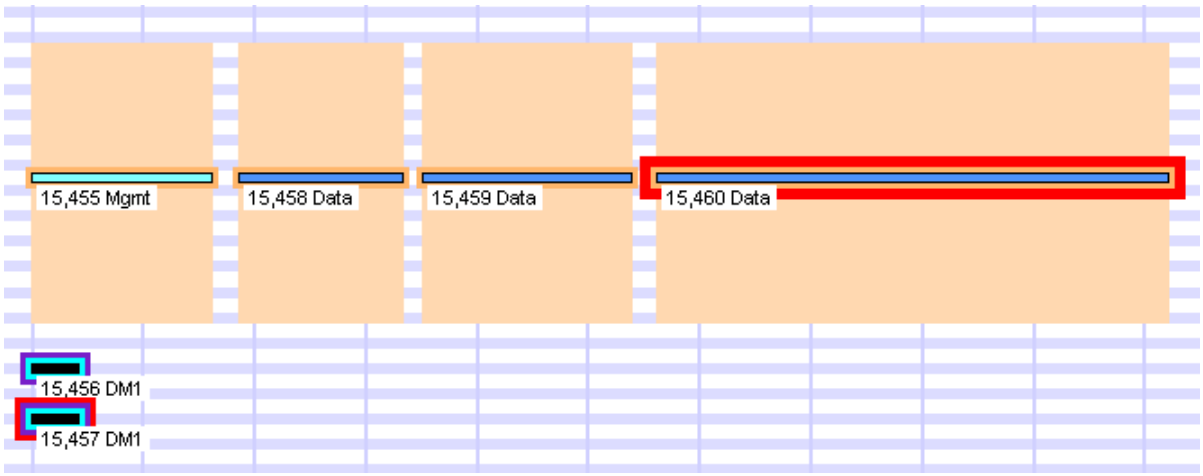


Figure 4.71 - Descriptive text on timeline packets.

Placing the mouse pointer on a packet displays a tooltip (color-coded by technology) that gives detailed information.

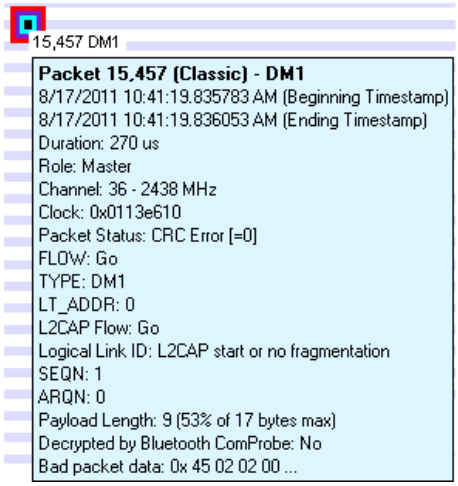

15,457 DM1
Packet 15,457 (Classic) - DM1
8/17/2011 10:41:19.835783 AM (Beginning Timestamp)
8/17/2011 10:41:19.836053 AM (Ending Timestamp)
Duration: 270 us
Role: Master
Channel: 36 - 2438 MHz
Clock: 0x0113e610
Packet Status: CRC Error [=0]
FLOW: Go
TYPE: DM1
LT_ADDR: 0
L2CAP Flow: Go
Logical Link ID: L2CAP start or no fragmentation
SEQN: 1
ARQN: 0
Payload Length: 9 (53% of 17 bytes max)
Decrypted by Bluetooth ComProbe: No
Bad packet data: 0x 45 02 02 00 ...

Figure 4.72 - A tool tip for a Classic *Bluetooth* packet.

4.4.2.28 Relocating the tool tip

You can relocate the tool tip for convenience or to see the timeline or throughput graph unobstructed while displaying packet information. In the **Format** menu select **Show Tooltips in Upper-Left Corner of Screen**, and any time you mouse-over a packet the tool tip will appear anchored in the upper-left corner of the computer screen. To return to viewing the tool tip adjacent to the packets deselect the tool tip format option in the menu.

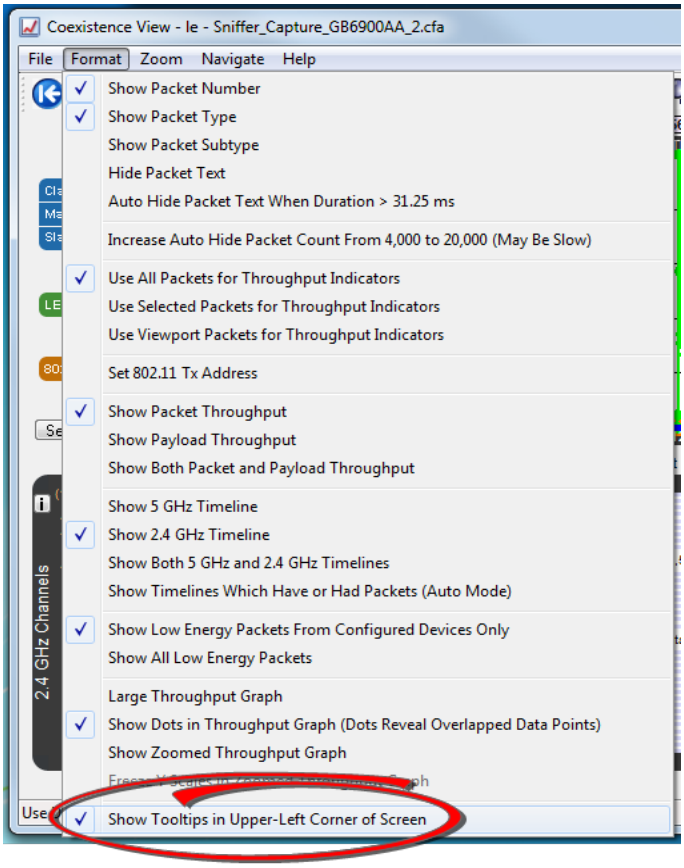

Coexistence View - Ie - Sniffer_Capture_GB6900AA_2.cfa
File
Format
Zoom
Navigate
Help
Show Packet Number
Show Packet Type
Show Packet Subtype
Hide Packet Text
Auto Hide Packet Text When Duration > 31.25 ms
Increase Auto Hide Packet Count From 4,000 to 20,000 (May Be Slow)
Use All Packets for Throughput Indicators
Use Selected Packets for Throughput Indicators
Use Viewport Packets for Throughput Indicators
Set 802.11 Tx Address
Show Packet Throughput
Show Payload Throughput
Show Both Packet and Payload Throughput
Show 5 GHz Timeline
Show 2.4 GHz Timeline
Show Both 5 GHz and 2.4 GHz Timelines
Show Timelines Which Have or Had Packets (Auto Mode)
Show Low Energy Packets From Configured Devices Only
Show All Low Energy Packets
Large Throughput Graph
Show Dots in Throughput Graph (Dots Reveal Overlapped Data Points)
Show Zoomed Throughput Graph
Show Tooltips in Upper-Left Corner of Screen
2.4 GHz Channels

Figure 4.73 - Coexistence View Format Menu - Show Tooltips on Computer Screen

Packet 15,455 (802.11) - Management - Beacon
8/17/2011 10:41:19.835783 AM (Beginning Timestamp)
8/17/2011 10:41:19.836799 AM (Ending Timestamp)
Radio Timestamp: n/a
Duration: 1.016 ms
Type: Management
Subtype: Beacon
Channel: 10 (2457 MHz)
Width: 20 MHz
Data Rate: 1.0 Mb/s
Channel Type: 802.11b
Packet Len: 128 bytes
Payload Len: 0 bytes
Source Address: Cisco-Linksys LLC 72:b3:a6 (SA)
Destination Address: ff:ff:ff:ff:ff:ff (DA)
tence View - bpa - (bt+le+wf) (hs) (18,842 packets).cfa
mat Zoom Navigate Spectrum Help
All Selected Viewport
Show Zoom
Avg throughput (bits/s)
1 sec throughput (bits/s)
width = 1 sec peak = 6,216
LE
width = 1 sec peak = 12,408
802.11
width = 1 sec peak = 246,072
Set
802.11 Tx: 00:00:00:22:21:bc
bits / s (2 s / point)
15,381
Selected Packet: 15,452

Figure 4.74 - Coexistence View Timeline Tool Tip Shown Anchored to Computer Screen

4.4.2.29 The two Timelines

There are two **Timelines** available for viewing, one for the 5 GHz range and one for the 2.4 GHz range. Classic *Bluetooth* and *Bluetooth* low energy occur only in the 2.4 GHz range. 802.11 can occur in both.

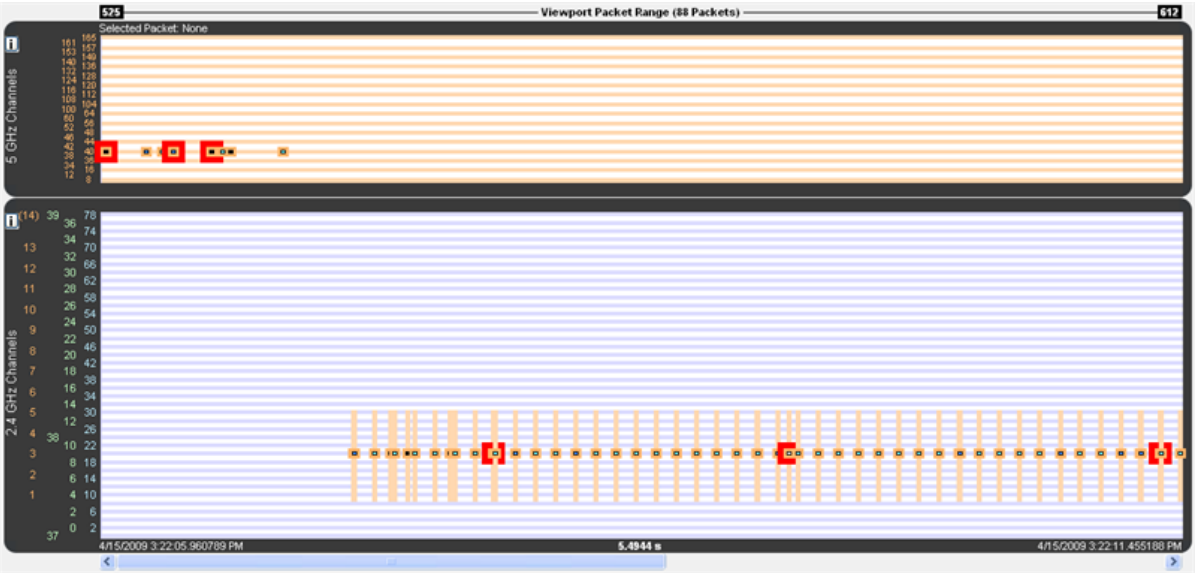


Figure 4.75 - 5 GHz and 2.4 GHz 802.11 packets

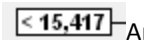
The y-axis labels show the channels for each technology and are color-coded: Blue = Classic *Bluetooth*, Green = *Bluetooth* low energy, Orange = 802.11.

The 5 GHz timeline has only 802.11 channel labels, and the rows alternate orange and white, one row per channel.

The 2.4 GHz timeline has labels for all three technologies. The rows alternate blue and white, one row per Classic *Bluetooth* channel. The labels going left-to-right are 802.11 channels, *Bluetooth* low energy advertising channels, *Bluetooth* low energy regular channels, and Classic *Bluetooth* channels.

The **Viewport Packet Range** above the timelines shows the packet range and packet count of packets that would be visible if both timelines were shown (i.e. hiding one of the timelines doesn't change the packet range or count). This packet range matches the packet range shown above the viewport in the Throughput Graph, as it must since the viewport defines the time range used by the timelines. When no packets are in the time range, each of the two packet numbers is drawn with an arrow to indicate the next packet in each direction and can be clicked on to navigate to that packet (the packet number changes color when the mouse pointer is placed on it in this case).

An arrow points to the next packet when no packets are in the time range.



An arrowed packet number changes color when the mouse pointer is on it. Clicking navigates to that packet.

The header shows information for packets that are selected.

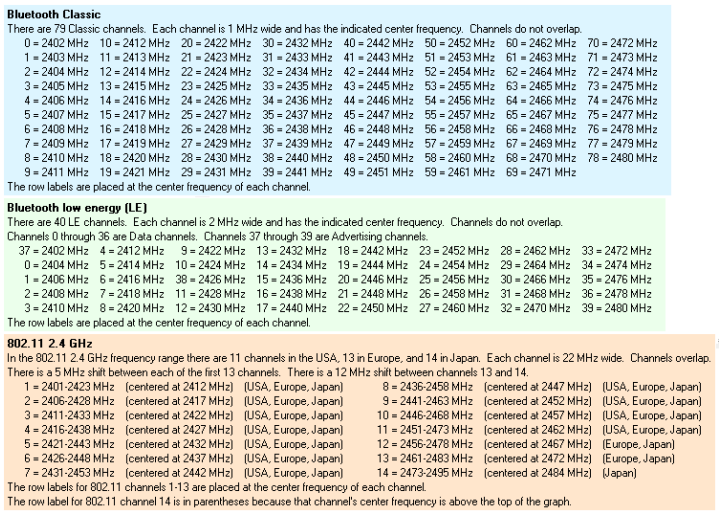
The footer shows the beginning/ending timestamps and visible duration of the timelines.

The 'i' buttons bring up channel information windows, which describe channel details for each technology. They make for interesting reading.

802.11 5 GHz

Only channels with a base value of 5 GHz and spacings of either 20 or 40 MHz are shown here. Due to space limitations, each channel is drawn with fixed spacing instead of being spaced relative to its distance from other channels as is done with 2.4 GHz channels (with the exception of 802.11 channel 14).

Figure 4.76 - 5 GHz information window



Bluetooth Classic

There are 79 Classic channels. Each channel is 1 MHz wide and has the indicated center frequency. Channels do not overlap.

0 = 2402 MHz	10 = 2412 MHz	20 = 2422 MHz	30 = 2432 MHz	40 = 2442 MHz	50 = 2452 MHz	60 = 2462 MHz	70 = 2472 MHz
1 = 2403 MHz	11 = 2413 MHz	21 = 2423 MHz	31 = 2433 MHz	41 = 2443 MHz	51 = 2453 MHz	61 = 2463 MHz	71 = 2473 MHz
2 = 2404 MHz	12 = 2414 MHz	22 = 2424 MHz	32 = 2434 MHz	42 = 2444 MHz	52 = 2454 MHz	62 = 2464 MHz	72 = 2474 MHz
3 = 2405 MHz	13 = 2415 MHz	23 = 2425 MHz	33 = 2435 MHz	43 = 2445 MHz	53 = 2455 MHz	63 = 2465 MHz	73 = 2475 MHz
4 = 2406 MHz	14 = 2416 MHz	24 = 2426 MHz	34 = 2436 MHz	44 = 2446 MHz	54 = 2456 MHz	64 = 2466 MHz	74 = 2476 MHz
5 = 2407 MHz	15 = 2417 MHz	25 = 2427 MHz	35 = 2437 MHz	45 = 2447 MHz	55 = 2457 MHz	65 = 2467 MHz	75 = 2477 MHz
6 = 2408 MHz	16 = 2418 MHz	26 = 2428 MHz	36 = 2438 MHz	46 = 2448 MHz	56 = 2458 MHz	66 = 2468 MHz	76 = 2478 MHz
7 = 2409 MHz	17 = 2419 MHz	27 = 2429 MHz	37 = 2439 MHz	47 = 2449 MHz	57 = 2459 MHz	67 = 2469 MHz	77 = 2479 MHz
8 = 2410 MHz	18 = 2420 MHz	28 = 2430 MHz	38 = 2440 MHz	48 = 2450 MHz	58 = 2460 MHz	68 = 2470 MHz	78 = 2480 MHz
9 = 2411 MHz	19 = 2421 MHz	29 = 2431 MHz	39 = 2441 MHz	49 = 2451 MHz	59 = 2461 MHz	69 = 2471 MHz	

The row labels are placed at the center frequency of each channel.

Bluetooth low energy (LE)

There are 40 LE channels. Each channel is 2 MHz wide and has the indicated center frequency. Channels do not overlap.
Channels 0 through 36 are Data channels. Channels 37 through 39 are Advertising channels.

37 = 2402 MHz	4 = 2412 MHz	9 = 2422 MHz	13 = 2432 MHz	18 = 2442 MHz	23 = 2452 MHz	28 = 2462 MHz	33 = 2472 MHz
0 = 2404 MHz	5 = 2414 MHz	10 = 2424 MHz	14 = 2434 MHz	19 = 2444 MHz	24 = 2454 MHz	29 = 2464 MHz	34 = 2474 MHz
1 = 2406 MHz	6 = 2416 MHz	38 = 2426 MHz	15 = 2436 MHz	20 = 2446 MHz	25 = 2456 MHz	30 = 2466 MHz	35 = 2476 MHz
2 = 2408 MHz	7 = 2418 MHz	11 = 2428 MHz	16 = 2438 MHz	21 = 2448 MHz	26 = 2458 MHz	31 = 2468 MHz	36 = 2478 MHz
3 = 2410 MHz	8 = 2420 MHz	12 = 2430 MHz	17 = 2440 MHz	22 = 2450 MHz	27 = 2460 MHz	32 = 2470 MHz	39 = 2480 MHz

The row labels are placed at the center frequency of each channel.

802.11 2.4 GHz

In the 802.11 2.4 GHz frequency range there are 11 channels in the USA, 13 in Europe, and 14 in Japan. Each channel is 22 MHz wide. Channels overlap.
There is a 5 MHz shift between each of the first 13 channels. There is a 12 MHz shift between channels 13 and 14.

1 = 2401-2423 MHz	(centered at 2412 MHz)	(USA, Europe, Japan)	8 = 2436-2458 MHz	(centered at 2447 MHz)	(USA, Europe, Japan)
2 = 2406-2428 MHz	(centered at 2417 MHz)	(USA, Europe, Japan)	9 = 2441-2463 MHz	(centered at 2452 MHz)	(USA, Europe, Japan)
3 = 2411-2433 MHz	(centered at 2422 MHz)	(USA, Europe, Japan)	10 = 2446-2468 MHz	(centered at 2457 MHz)	(USA, Europe, Japan)
4 = 2416-2438 MHz	(centered at 2427 MHz)	(USA, Europe, Japan)	11 = 2451-2473 MHz	(centered at 2462 MHz)	(USA, Europe, Japan)
5 = 2421-2443 MHz	(centered at 2432 MHz)	(USA, Europe, Japan)	12 = 2456-2478 MHz	(centered at 2467 MHz)	(Europe, Japan)
6 = 2426-2448 MHz	(centered at 2437 MHz)	(USA, Europe, Japan)	13 = 2461-2483 MHz	(centered at 2472 MHz)	(Europe, Japan)
7 = 2431-2453 MHz	(centered at 2442 MHz)	(USA, Europe, Japan)	14 = 2473-2495 MHz	(centered at 2484 MHz)	(Japan)

The row labels for 802.11 channels 1-13 are placed at the center frequency of each channel.
The row label for 802.11 channel 14 is in parentheses because that channel's center frequency is above the top of the graph.

Figure 4.77 - 2.4 GHz information windows

4.4.2.30 *Bluetooth* slot markers

When zoomed in far enough *Bluetooth* slot markers appear in the 2.4 GHz timeline. A *Bluetooth* slot is 625 µs wide.

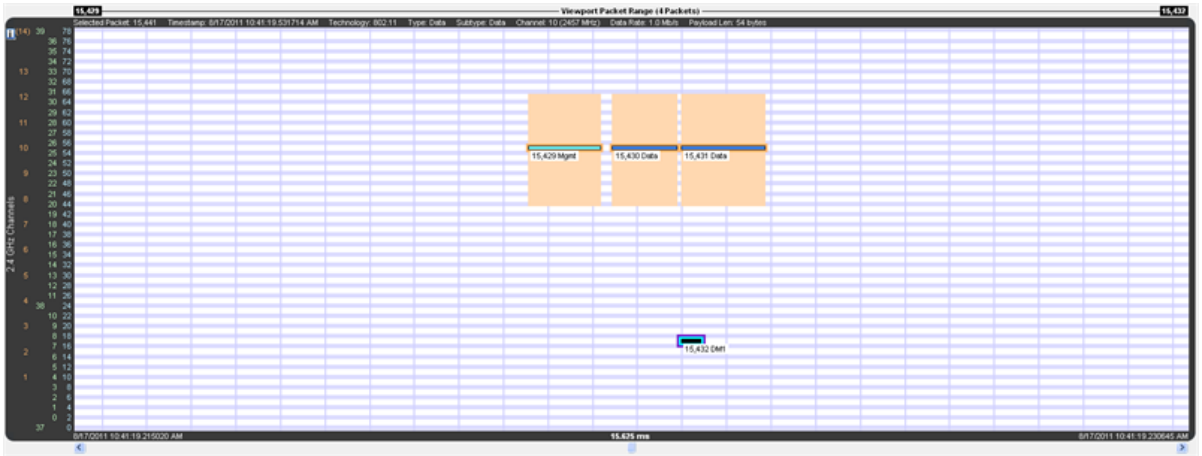


Figure 4.78 - Vertical blue lines are *Bluetooth* slot markers

4.4.2.31 Zooming

There are various ways to zoom:

1. Drag one of the sides of the **Throughput Graph** viewport.
2. Select a zoom preset from the **Zoom** or right-click menus.
3. Select the **Zoom In** or **Zoom Out** button or menu item.
4. Turn the mouse wheel in the **Timelines** or the **Zoomed Throughput Graph** while the zoom cursor is selected. The action is the same as selecting the **Zoom In** and **Zoom Out** buttons and menu items except that the time point at the mouse pointer is kept in place if possible.
5. Select the **Zoom to Data Point Packet Range** menu item, which zooms to the packet range shown in the most recently displayed tool tip.
6. Select the **Zoom to Selected Packet Range** menu item, which zooms to the selected packet range as indicated in the **Selected Packets** text in the timeline header.
7. Select the **Custom Zoom** menu item. This is the zoom level from the most recent drag of a viewport side, selection of **Zoom to Data Point Packet Range**, or selection of **Zoom to Selected Packet**.

The zoom buttons and tools step through the zoom presets and custom zoom, where the custom zoom is logically inserted in value order into the zoom preset list for this purpose.

4.4.2.32 Discontinuities

A discontinuity is when the timestamp going from one packet to the next either goes backward by any amount or forward by more than 4.01 s (this value is used because the largest possible connection interval in *Bluetooth* low energy is 4.0 s). A discontinuity is drawn as a vertical cross-hatched area one *Bluetooth* slot (625 µs) in width. A discontinuity for a timestamp going backward is called a negative discontinuity and is shown in red. A discontinuity for a timestamp going forward by more than 4.01 s is called a positive discontinuity and is shown in black. A positive discontinuity is a cosmetic nicety to avoid lots of empty space. A negative discontinuity is an error.

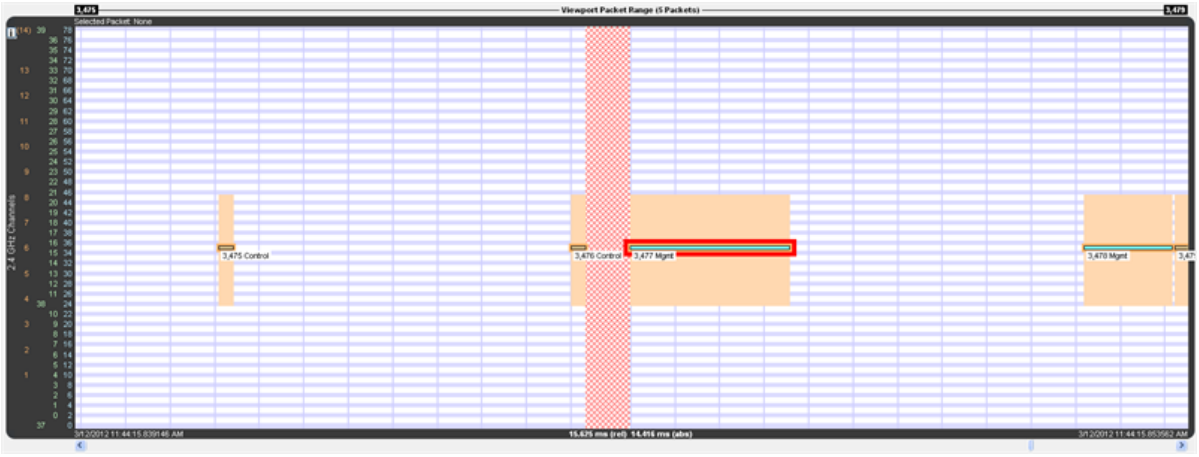


Figure 4.79 - A negative discontinuity

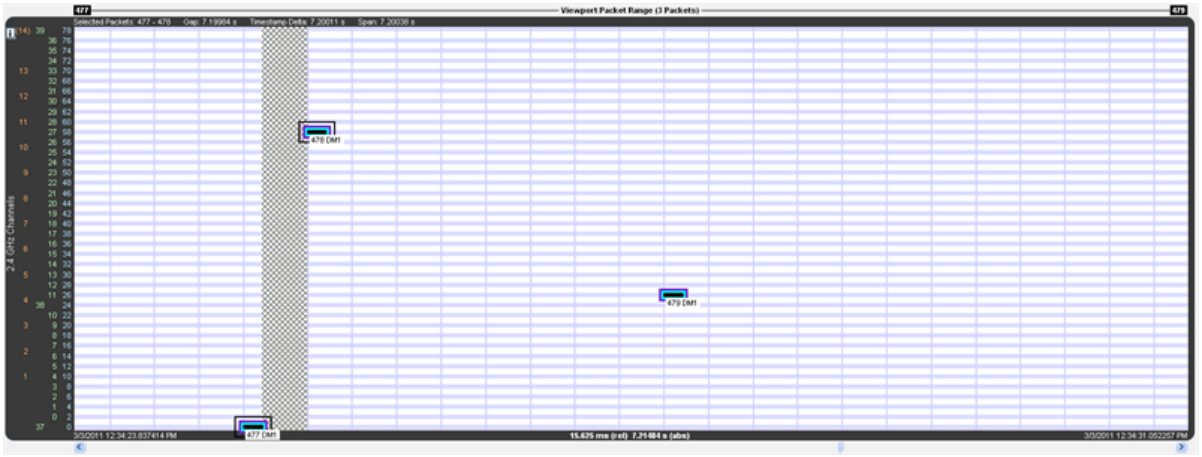


Figure 4.80 - A positive discontinuity

When there are one or more discontinuities the actual time encompassed by the visible timeline differs from the zoom level duration that would apply in the absence of any discontinuities. The actual time, referred to as absolute time, is shown followed by "(abs)". The zoom level duration, referred to as relative time, is shown followed by "(rel)". When there are no discontinuities, relative and absolute time are the same and a single value is shown.

Figure 4.81 - Timeline header with discontinuity

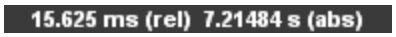


Figure 4.82 - Timeline duration footer with discontinuity

For example, the timeline above has a zoom level duration of 15.625 ms (the relative time shown in the footer). But the discontinuity graphic consumes the width of a *Bluetooth* slot (625 µs), and that area is 7.19984 s of absolute time as shown by the Gap value in the header. So the absolute time is 7.21484 s:

Zoom level duration – *Bluetooth* slot duration + Gap duration =

15.625 ms - 625 µs + 7.19984 s =

0.015625 s – 0.000625 s + 7.199840 s =

0.015000 s + 7.199840 s =

7.214840 s =

7.21484 s

4.4.2.33 High-Speed *Bluetooth*

High-speed *Bluetooth* packets, where *Bluetooth* content hitches a ride on 802.11 packets, have a blue frequency range box instead of orange as with regular 802.11 packets (both are shown below), and the tool tip has two colors, orange for 802.11 layers and blue for *Bluetooth* layers.

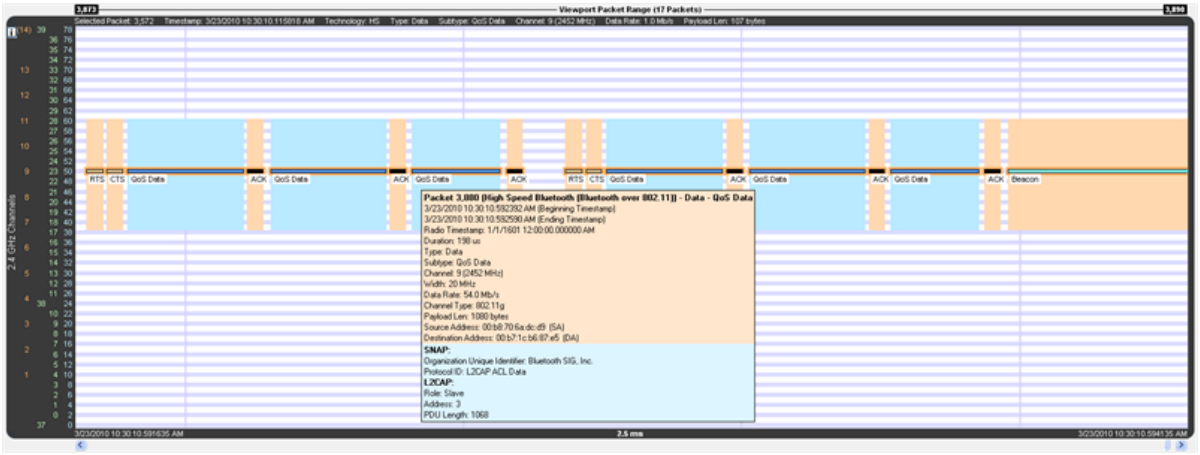


Figure 4.83 - High-speed *Bluetooth* packets have a blue frequency box and a two-tone tool tip

4.4.2.34 Coexistence View - No Packets Displayed with Missing Channel Numbers

Note: This topic applies only to Classic *Bluetooth*.

Captured packets that don't contain a channel number, such as HCI and BTSnoop, will not be displayed. When no packets have a channel number the **Coexistence View Throughput Graph** and **Timelines** will display a message: "Packets without a channel number (such as HCI) won't be shown."

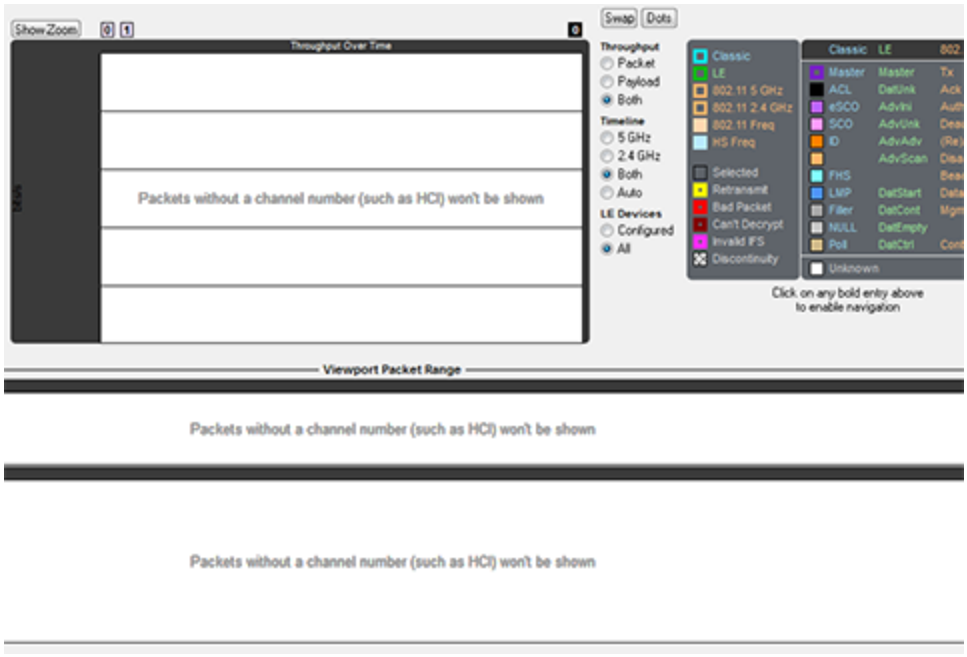


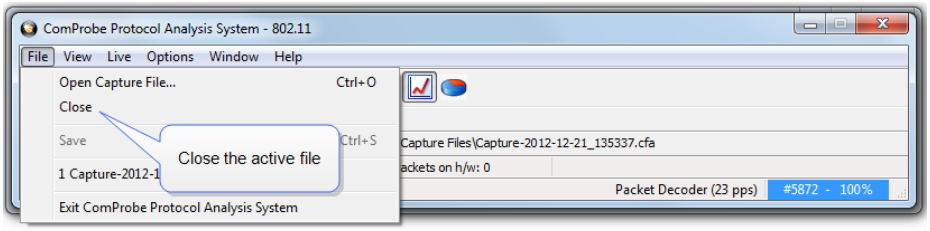
Figure 4.84 - Missing Channel Numbers Message in Timelines

4.4.2.35 High Speed Live View

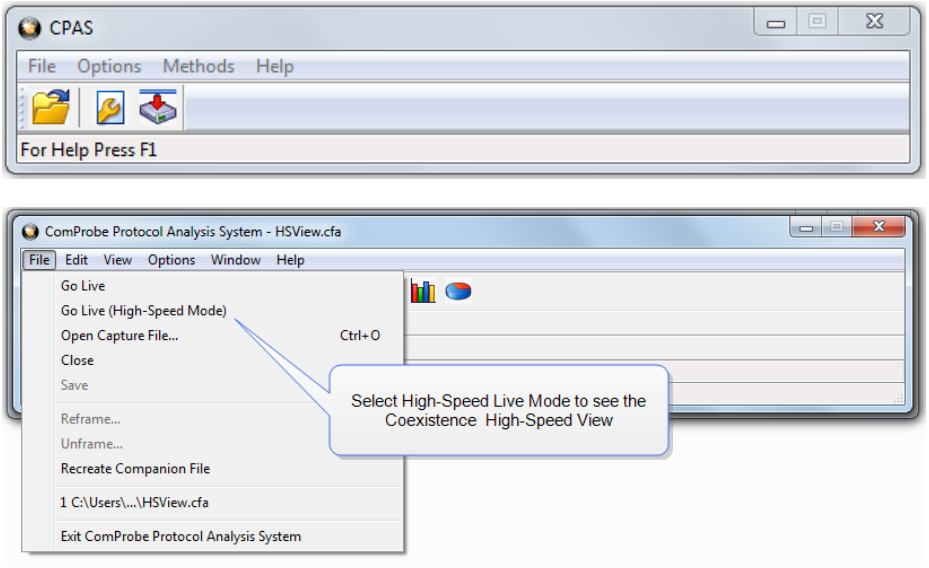
When using the ComProbe 802.11 in conjunction with other ComProbe devices, or in a stand-alone configuration, a smaller version of the standard **Coexistence View** is available. This **High Speed Live View** is essentially the **Viewport** from the standard **Coexistence View**.

When viewing **High Speed Live**, only 802.11 traffic is visible. Because Bluetooth® packets are slow they are not visible in High Speed mode.

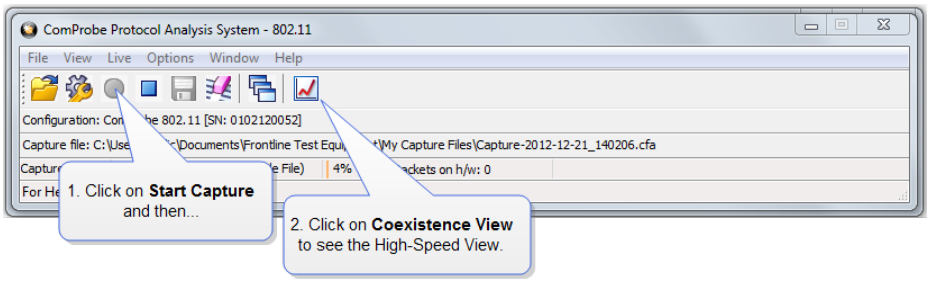
1. Click on the **Control** window **File** menu and select **Close**.



2. The **Control** window will open again. Click on the Control Window **File** menu and select **Go Live (High-Speed Mode)**



3. Click on the **Control** window **Start Capture** button to begin capturing data. Click on the **Coexistence View** button and the **High-Speed View** will appear.


ComProbe Protocol Analysis System - 802.11
File View Live Options Window Help
1. Click on Start Capture and then...
2. Click on Coexistence View to see the High-Speed View.

The Coexistence View (High Speed Live Mode) window will appear.

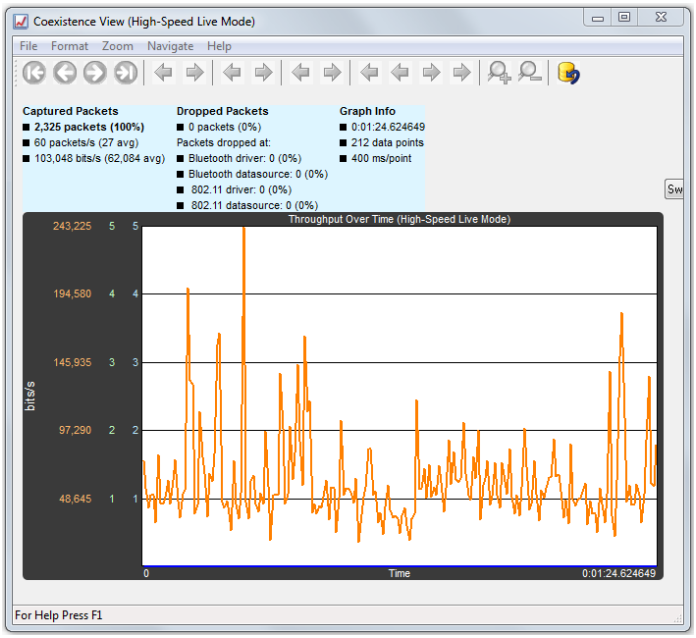


Figure 4.12 High-Speed Live Window

4.5 Data/Audio Extraction

You use Data/Audio Extraction to pull out data from various decoded Bluetooth® protocols. Once you have extracted the data, you can save them into different file types, such as text files, graphic files, email files, .mp3 files, and more. Then you can examine the specific files information individually.

1. You access this dialog by selecting Extract Data/Audio from the View menu or by clicking on the icon from the toolbar .

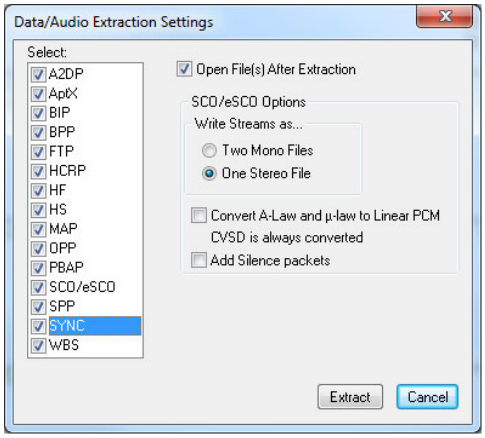


Figure 4.13 Data/Audio Extraction Settings dialog

2. Choose a checkbox(es) on the left side of the dialog to identify from which profile(s) you want to extract data.

   It's important to note that if there is no data for the profile(s) you select, no extracted file is created.

3. If you want the file(s) to open automatically after they are extracted, select the **Open File(s) After Extraction** checkbox.

   Note: This does not work for SCO/eSCO.

4. Click on a radio button to write the streams as **Two Mono Files** or as **One Stereo File**.

   Note: This option is for SCO/eSCO only.

5. Select the checkbox if you want to convert **A-Law and μ-law to Linear PCM.**
   CVSD are always converted to Linear PCM. It's probably a good idea to convert to Linear PCM since more media players accept this format.

   Note: This option is for SCO/eSCO only.

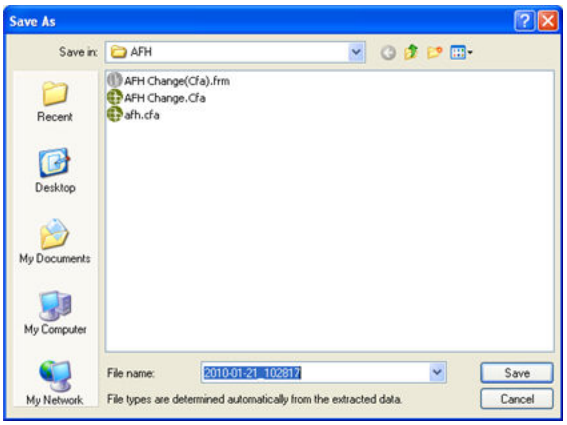
6. Select the **Add Silence packets** to insert the silence packets (dummy packets) for the reserved empty slots into the extracted file. If this option is not selected, the audio packets are extracted without inserting the silence packets for the reserved empty slots.

   Note: This option is for SCO/eSCO only.

7. Select **Extract.**

   A **Save As** dialog appears.

   The application will assign a file name and file type for each profile you select in Step 1 above. The file type varies depending on the original profile. A separate file for each profile will be created, but only for those profiles with available data.



8. Select a location for the file.

9. Click **Save**.

   The **Data Extraction Status** and **Audio Extraction Status** dialogs appear. When the process is complete the dialogs display what files have been created and where they are located.

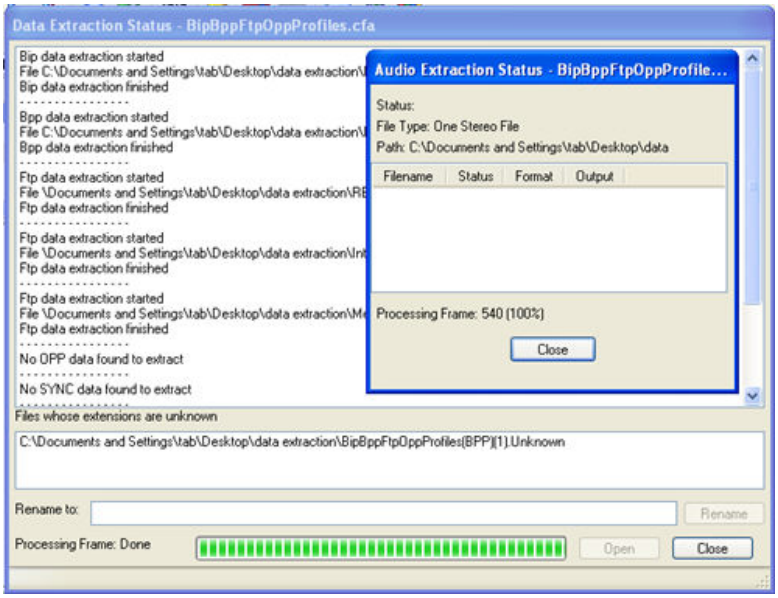


Figure 4.14 Data and Audio Extraction Status

   If you selected **Open Files(s) After Extraction**, the files open automatically.

10. If you did not select this option, you can open a file by simply double-clicking on the name.

Also, if a file type is unknown, you can select the file and it appears in the **Rename to**: text box.

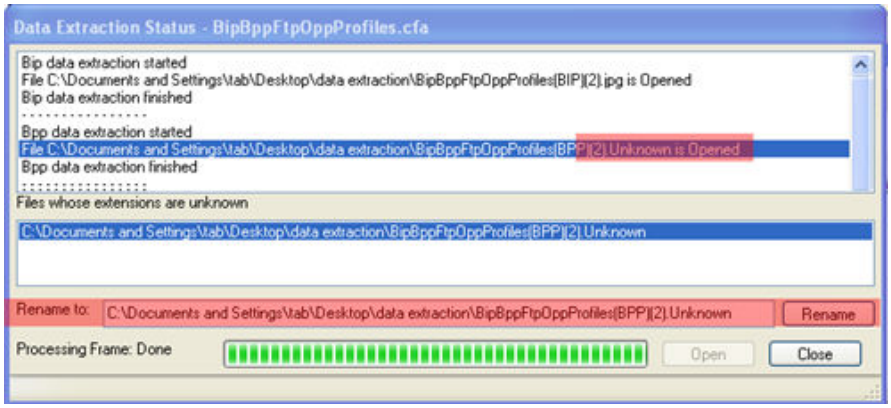


Figure 4.15 Rename To in the bottom section of Data Extraction Status

Then you can rename the file, adding a file type to attempt to open the file.

When you are finished, select **Close** to close the dialogs.

4.6 Statistics

4.6.1 Statistics Window

The Statistics window supplies basic information about the data on the network. When reviewing a capture file, the **Statistics** window shows a summary of the data in the file.

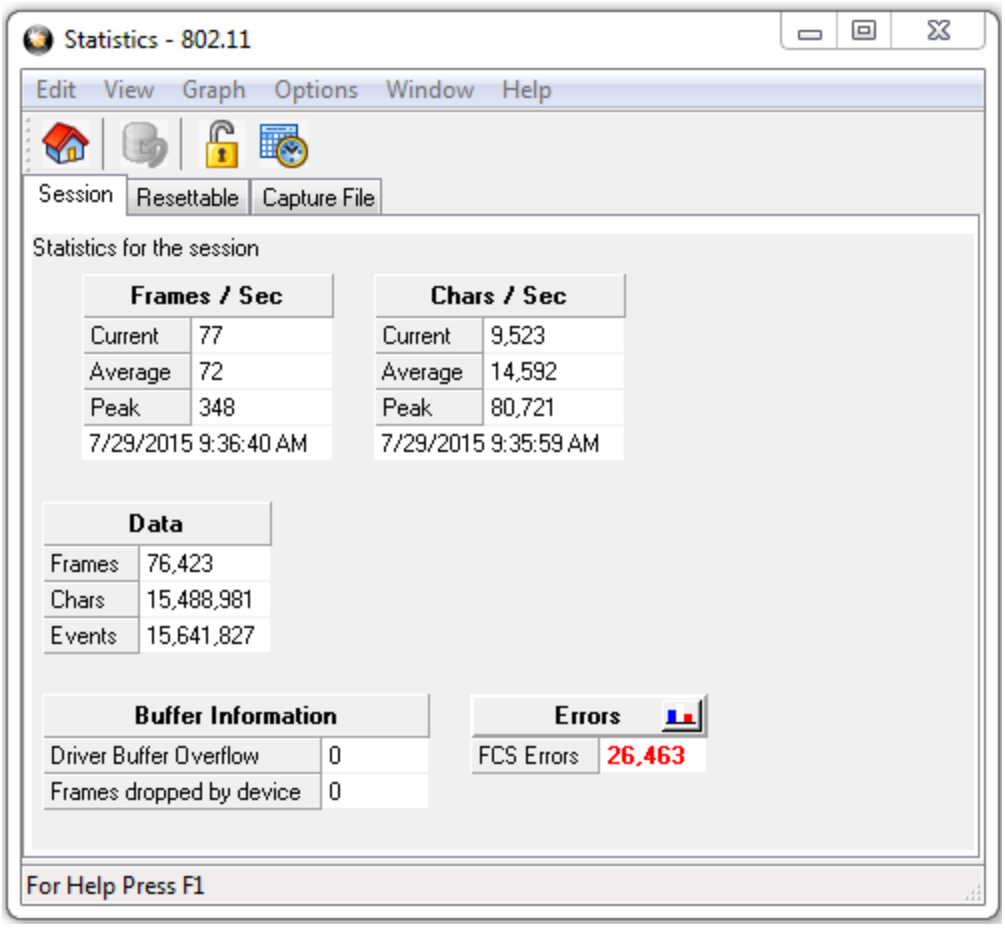


Figure 4.85 - 802.11 Statistics Window

To open the **Statistics** window, click the Statistics icon on the **Control** window toolbar, or choose **Statistics** from the **View** menu on the **Control** window.

The analyzer monitors the network and collects statistics all the time, even when data is not actively being captured. Activate the **Lock** icon to stop the window from updating. Click the **Unlock** icon again to resume updating. The analyzer continues to monitor network traffic while the **Statistics** window is locked, so you may see the numbers jump right after updating has resumed, reflecting all the statistics that were gathered while the window was locked.

Statistics Window Menus

Table 4.16 - 802.11 Statistics Window Menus

Menu	Selection	Description
Edit	**Copy All To Clipboard**	Copies all statistics to the Windows clipboard.
	Notes	Opes the notes dialog for recording comments on a capture file. Only available when view a capture file.
	Copy Chars/Sec To Clipboard	Copies the character rate statistics to the Windows clipboard.
	Copy Data To Clipboard	Copies data statistics to the Windows clipboard.
	Copy Errors To Clipboard	Copies only the FSC error statistics to the Windows clipboard.
	Copy Buffer To Clipboard	Copies only the data currently in the buffer to the Windows Clipboard.
	Copy Frames/Sec To Clipboard	Copies the frame rate statistics to the Windows clipboard
View	**Control Window**	When checked will open the window or Statistics Window bar. When not checked, the window or bar is closed.
	Event Display	
	Frame Display	
	Toolbar	
	Status Bar	
	Toggle Display Lock	When checked, the displayed statistics will stop updating, although data is still being captured. Unchecking will resume statistics updating.
	Reset	Available during live capture. Resets all displayed statistics and restarts the calculations.
Graph	**Graph Errors...**	Opens the Errors 802.11 window.
Options	**I/O Settings...**	Performs the same function as the control Window Options Menu, I/O Settings
	Set Timestamping Format	Opens the Timestamping Options window that allows for changing the resolution of the timestamps.
	Change the Font Size	Opens a pop-up with font size selections.
Window	**Close Window**	Closes the Statistics Window
	ComProbe Protocol Analysis System	Clicking on these selections will change the focus from the Statistics Window to the selected window.
	Statistics	
	Errors	
Help	**Help Topics**	Opens the ComProbe Help window.

Table 4.16 - 802.11 Statistics Window Menus (continued)

Menu	Selection	Description
	About ComProbe Protocol Analysis System	Provides a pop-up showing the version and release information, Frontline contact information, and copyright information.
	Support on the Web	Opens a browser to fte.com technical support page.

Statistics Window Toolbar

Statistics Window Toolbar Icons

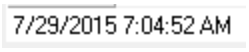
Icon	Description
	Changes the focus to the Control Window
	Reset the statistics tables
	Display Lock/Unlock
	Timestamp Format

4.6.2 Session, Resettable and Capture File Tabs

The **Session**, **Resettable**, and **Capture File** tabs are parts of the **Statistics** and **Errors** windows.

Information about all data collected since the analyzer was started is shown in the **Session** tab. The **Session** tab cannot be reset; in this sense, it is like the odometer on a car. The odometer on a car shows you all the miles driven since the car was built, and the **Session** tab shows you all the data collected since the analyzer was started.

If you think of the **Session** tab as the odometer, then the **Resettable** tab is the trip odometer. It can be reset, and allows you to record statistics for a new "trip". In this way you can effectively start a new session without having to restart the analyzer. If the **Reset** button was pressed during the capture, then the numbers on this tab differs from the numbers on the Session tab.



The timestamp appearing in **Session** tab fields is the timestamp of when the analysis began. The timestamp appearing in the **Resettable** tab fields is the timestamp either when the analysis began or when the last Reset was initialted.

The **Capture File** tab shows information on the data that is currently in the capture. If the capture file had become full, the analyzer began to overwrite the oldest data and put new data in its place. This is called "wrapping". If the file wrapped, the numbers on the **Capture File** tab is smaller than those on the Session tab.

Occasionally some of the statistics read "n/a", for Not Available. This happens for various reasons. For example, many of the items on the **Capture File** tab become not available if the buffer becomes full and wraps. When this happens, the analyzer can no longer provide accurate statistics for the data in the file, because some of the data that the statistics are based on has been lost.

4.6.3 Copying Statistics To The Clipboard

Any table in the **Statistics** window can be copied to the clipboard where it can be pasted into any application.

1. Choose the name of the table from the **Edit** menu.
2. To copy the contents of all the tables, choose **Copy All to Clipboard**.

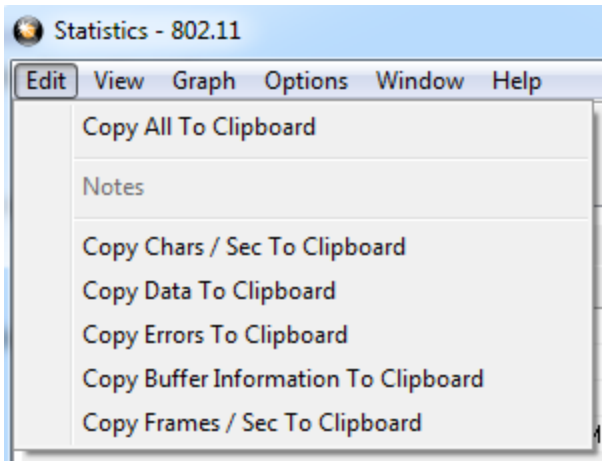
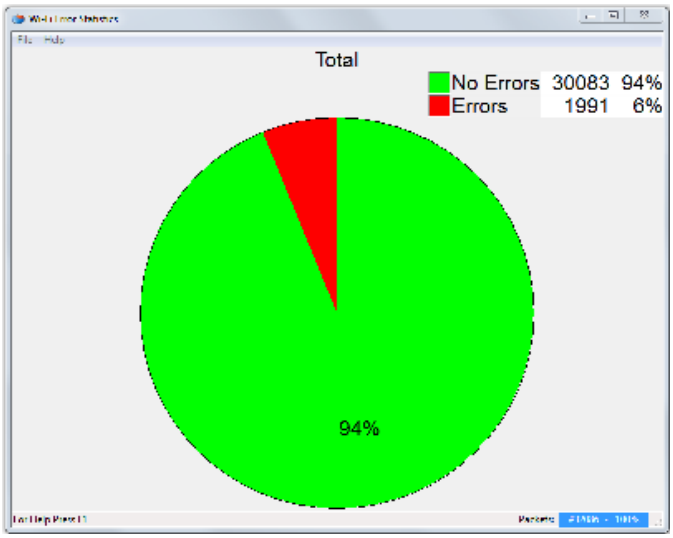


Figure 4.86 - 802.11 Edit Menu for Copying

4.6.4 802.11 Error Statistics

The **Wi-Fi Error Statistics** window appears when you select the window from the icon in the **Control** window toolbar or the **Frame Display** toolbar. The dialog is view only; there is no user interaction possible.

The window displays the percentage of packets with and without errors in a pie chart and in a table.



4.6.5 Graphs

4.6.5.1 Statistics Errors Graphs

Open the **Statistics** window and click on the picture of a graph on the Errors table header, or choose the graph name from the Graph menu on the **Statistics** window.

The **Frame Sizes Graph** window has Session, Resettable and Capture File tabs that correspond to the tabs on the **Statistics** window. Each tab shows the data that corresponds to the appropriate tab on the **Statistics** window.

The window displays the errors in either a pie chart or bar graph format. Click the **Pie** icon to display a pie chart, and click the Bar icon to display a bar graph.

4.6.5.2 Printing Error Graphs

Click the **Print** icon to print the graph. The analyzer prints exactly what is shown in the window.

Chapter 5 Navigating and Searching the Data

The following sections describe how to navigate through the data and how to find specific data or packet conditions of interest to the user.

5.1 Find

Capturing and decoding data within the ComProbe analyzer produces a wealth of information for analysis. This mass of information by itself, however, is just that, a mass of information. There has to be ways to manage the information. ComProbe software provides a number of different methods for making the data more accessible. One of these methods is **Find**.

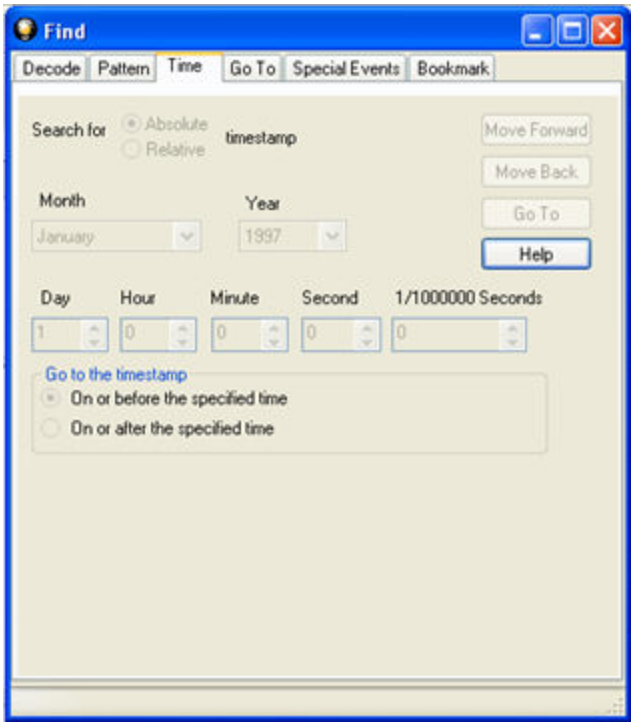


Figure 5.1 - Find Dialog

Find, as the name suggests, is a comprehensive search function that allows users to search for strings or patterns in the data or in the frame decode. You can search for errors, control signal changes, bookmarks, special events, time, and more. Once the information is located, you can easily move to every instance of the Find results.

5.1.1 Searching within Decodes

Searching within decodes lets you to do a string search on the data in the **Decode Pane** of the **Frame Display** window.

To access the search within decodes function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Decode** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

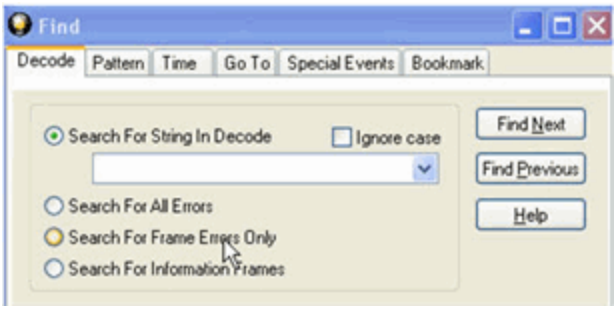


Figure 5.2 - Find Decode Tab Search for String

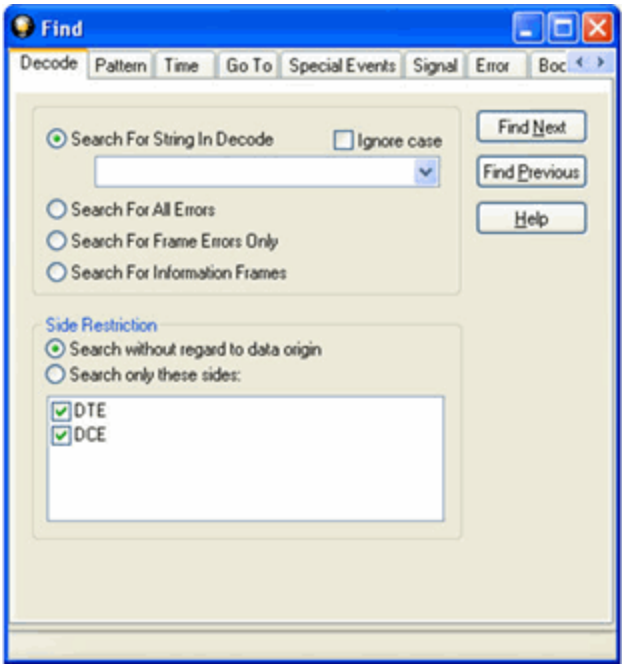


Figure 5.3 - Find Decode Tab Side Restriction

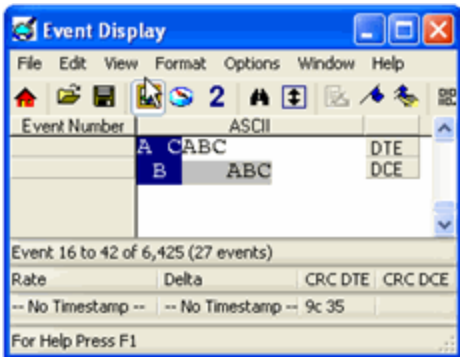
There are several options for error searching on the **Decoder** tab.

- **Search For String in Decoder** allows you to enter a string in the text box. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string. Every time you type in a search string, the analyzer saves the search. The next time you open **Find**, the drop-down list will contain your search parameters.
- **Search for All Errors** finds frame errors as well as frames with byte-level errors (such as parity or CRC errors).
- **Search for Frame Errors Only** finds frame specific errors, such as frame check errors.
- **Search for Information Frame** only searches information frames.

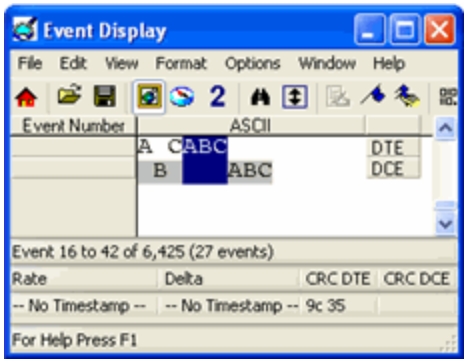
1. Enter the search string.
2. Check **Ignore Case** to do a case-insensitive search.
3. When you have specified the time interval you want to use, click on the **Find Next** or **Find Previous** buttons to start the search from the current event.

The result of the search is displayed in the **Decode** pane in **Frame Display.**

Side Restrictions - **Side Restriction** means that the analyzer looks for a pattern coming wholly from the DTE or DCE side. If you choose to search without regard for data origin, the analyzer looks for a pattern coming from one or both sides. For example, if you choose to search for the pattern ABC and you choose to search without regard for data origin, the analyzer finds all three instances of ABC shown here.



The first pattern, with the A and the C coming from the DTE device and the B coming from the DCE is a good example of how using a side restriction differs from searching without regard to data origin. While searching without regard for data origin finds all three patterns, searching using a side restriction never finds the first pattern, because it does not come wholly from one side or the other.



If you choose to search for the pattern ABC, and you restrict the search to just the DTE side, the analyzer finds the following pattern:

In this example, the analyzer finds only the second pattern (highlighted above) because we restricted the search to just the DTE side. The first pattern doesn't qualify because it is split between the DTE and DCE sides, and the third pattern, though whole, comes from just the DCE side.

If we choose both the DTE and the DCE sides in the above example, then the analyzer finds the second pattern followed by the third pattern, but not the first pattern. This is because each side has one instance in which the whole pattern can be found. The analyzer completely searches the DTE side first, followed by the DCE side.

Note: Side Restriction is available for pattern and error searching.

1. Select one of the two options.
2. Select **DTE**, **DCE**, or both.
3. When you made your selections, click on the **Find Next** or **Find Previous** buttons to start the search from the current event.

The result of the search is displayed in the **Decode** pane in **Frame Display.**

5.1.2 Searching by Pattern

Search by Pattern lets you perform a traditional string search. You can combine any of the formats when entering your string, and your search can include wildcards.

To access the search by pattern function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.

3. Click on the **Find** icon or choose **Find** from the **Edit** menu.

4. Click on the **Pattern** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

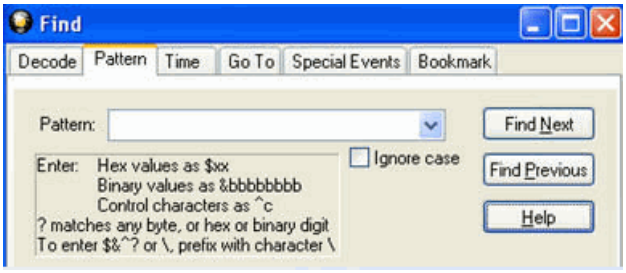


Figure 5.4 - Find Pattern Tab

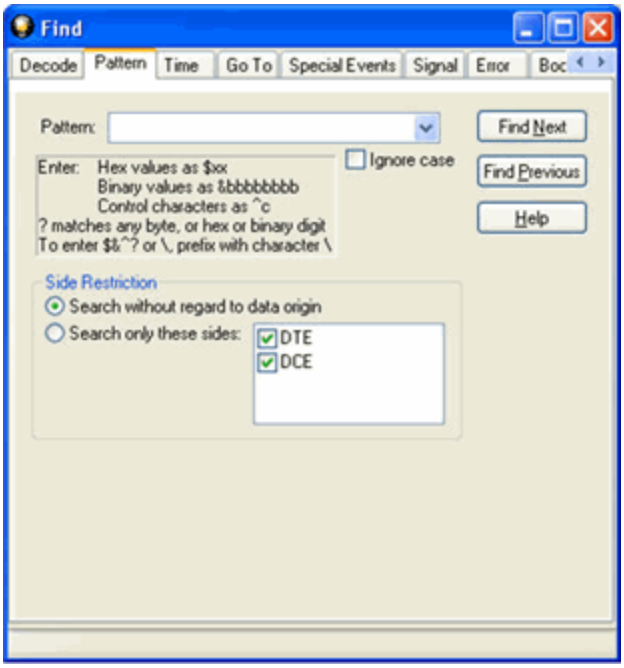


Figure 5.5 - Find Pattern Tab Side Restrictions

Pattern allows you to enter a string in the text box. You can use characters, hex or binary digits, control characters, wildcards or a combination of any of the formats when entering your string. Every time you type in a search string, the ComProbe analyzer saves the search. The next time you open **Find**, the drop-down list will contain your search parameters.

1. Enter the search pattern.

2. Check **Ignore Case** to do a case-insensitive search.

3. When you have specified the pattern you want to use, click on the **Find Next** or **Find Previous** buttons to start the search from the current event.

The result of the search is displayed in the in Frame Display and Event Display.

Refer to Searching by Decode on page 140 for information on **Side Restrictions**

5.1.3 Searching by Time

Searching with **Time** allows you search on timestamps on the data in **Frame Display** and **Event Display** window.

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Time** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

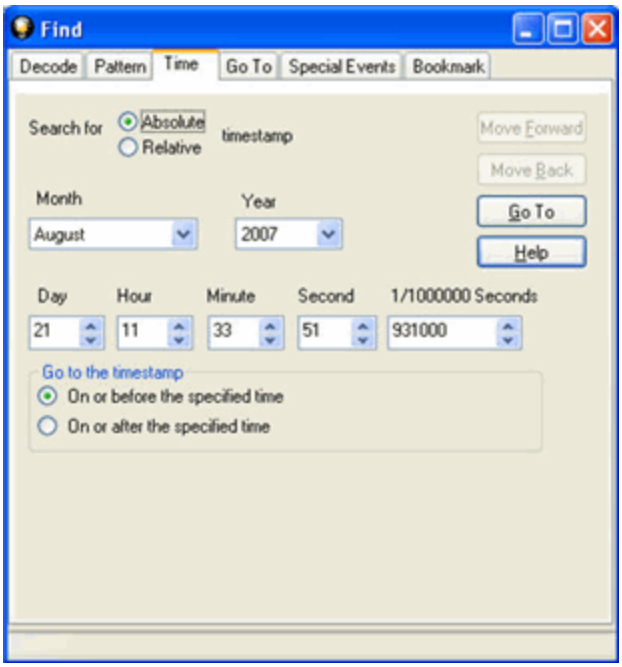


Figure 5.6 - Find by Time tab

The analyzer can search by time in several different ways.

Search for Absolute/Relative timestamp.

- Absolute - An absolute timestamp search means that the analyzer searches for an event at the exact date and time specified. If no event is found at that time, the analyzer goes to the nearest event either before or after the selected time, based on the "Go to the timestamp" selection.
- Relative - A relative search means that the analyzer begins searching from whatever event you are currently on, and search for the next event a specific amount of time away.

1. Select **Absolute** or **Relative**
2. Select the date and time using the drop-down lists for **Month**, **Year**, **Day**, **Hour**, **Minute**, **Second**, 1/**10000000**.

Note: Month and Year are not available if you select Relative.

3. When you have specified the time interval you want to use, click on the **Go To**, **Move Forward** or **Move Backward** buttons to start the search from the current event.

Note: When you select **Absolute** as **Search for**, **Go To** is available. When you select **Relative** as **Search for**, **Move Forward** or **Move Backward**is available.

Go to the timestamp: On or before/ On or after

The analyzer searches for an event that matches the time specified. If no event is found at the time specified, the analyzer goes to the nearest event either before or after the specified time. Choose whether to have the analyzer go to the nearest event before the specified time or after the specified time by clicking the appropriate radio button in the **Go to the timestamp** box.

If you are searching forward in the buffer, you usually want to choose the **On or After** option. If you choose the **On or Before** option, it may be that the analyzer finishes the search and not move from the current byte, if that byte happens to be the closest match.

When you select **Absolute** as **Search for**, the radio buttons are **On or before the specified time** or **On or after the specified time**. When you select **Relative** as **Search for**, the radio buttons are **On or before the specified time relative to the first selected item** or **On or after the specified time relative to the last selected item.**

1. Select **On or before the specified time** or **On or after the specified time**.
2. When you have specified the time interval you want to use, click on the **Go To**, **Move Forward** or **Move Backward** buttons to start the search from the current event.

   When you select **Absolute** as **Search for**, **Go To** is available. When you select **Relative** as **Search for**, **Move Forward** or **Move Backward**is available.

There are a couple of other concepts to understand in respect to searching with timestamps.

- The analyzer skips some special events that do not have timestamps, such as frame markers. Data events that do not have timestamps because timestamping was turned off either before or during capture are also skipped.

- Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.
- The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

5.1.4 Using Go To

Searching with Go To allows you to go to a particular frame or event, or to move through the data X number of events or frames at a time. You can move either forward or backwards through the data.

To access the Go To function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Go To** tab of the **Find** dialog.
5. The system displays the **Find** dialog with the **Go To** tab selected.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

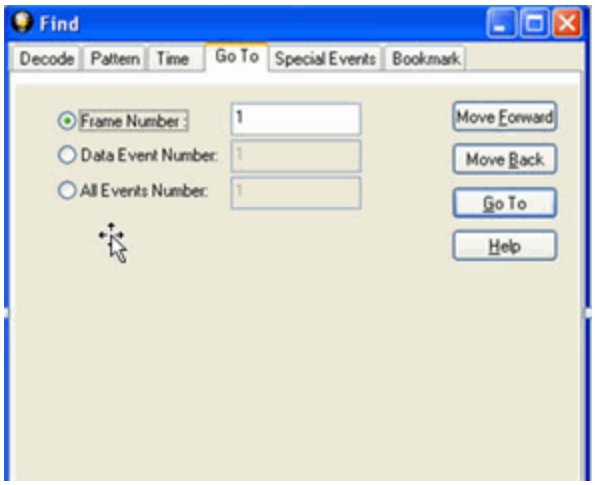


Figure 5.7 - Find Go To tab

To go to a particular frame :

1. Select the **Frame Number** radio button
2. Type the frame number in the box.
3. Click the **Go To** button.

4. To move forward or backward a set number of frames, type in the number of frames you want to move
5. Then click the **Move Forward** or **Move Back** button.

To go to a particular event :

1. Select the **Data Event Number** or **All Events Number** radio button.
2. Type the number of the event in the box.
3. Click the **Go To** button.
4. To move forward or backwards through the data, type in the number of events that you want to move each time.
5. Then click on the **Move Forward** or **Move Backward** button.
6. For example, to move forward 10 events, type the number 10 in the box, and then click on **Move Forward**. Each time you click on **Move Forward,** Frontline moves forward 10 events.

See Event Numbering for why the **Data Event Number** and **All Events Number** may be different. As a general rule, if you have the **Show All Events** icon depressed on the **Event Display** window or **Frame Display Event** pane, choose **All Events Number**. If the **Show All Events** button is up, choose **Data Event Number**.

5.1.5 Searching for Special Events

Frontline inserts or marks events other than data bytes in the data stream. For example, the analyzer inserts start-of-frame and end-of-frame markers into framed data, marking where each frame begins and ends. If a hardware error occurs, the analyzer shows this using a special event marker. You can use Find to locate single or multiple special events.

To access the search for special events function:

1. Open a capture file to search.
2. Open the Event Display or Frame Display window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Special Events** tab of the Find dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

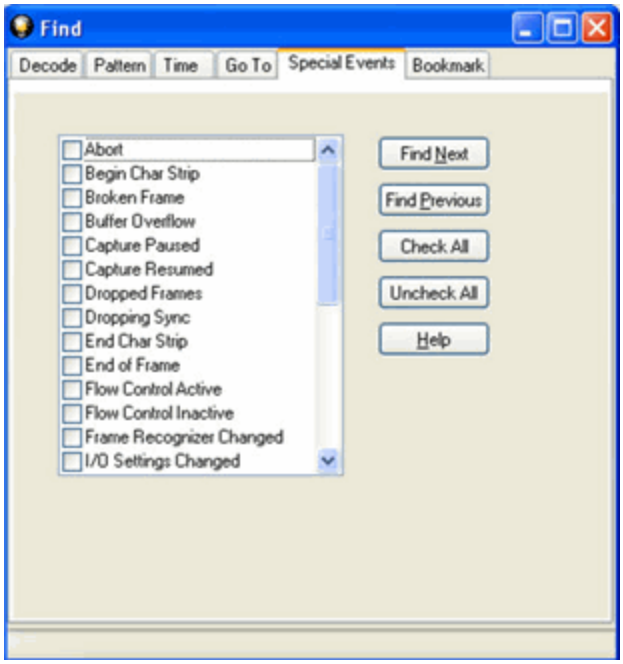


Figure 5.8 - Find Special Events tab

5. Check the event or events you want to look for in the list of special events. Use **Check All** or **Uncheck All** buttons to make your selections more efficient.
6. Click Find Next and Find Previous to move to the next instance of the event.

Not all special events are relevant to all types of data. For example, control signal changes are relevant only to serial data and not to Ethernet data.

For a list of all special events and their meanings, see List of all Event Symbols on page 58.

5.1.6 Searching by Signal

Searching with Signal allows you to search for changes in control signal states for one or more control signals. You can also search for a specific state involving one or more control signals, with the option to ignore those control signals whose states you don't care about.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where control signals changed.

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Signal** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

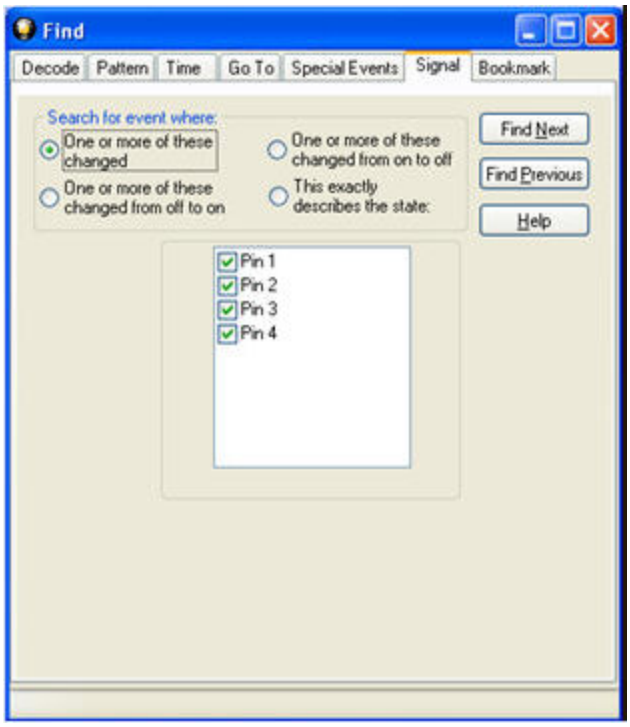


Figure 5.9 - Find Signal tab.

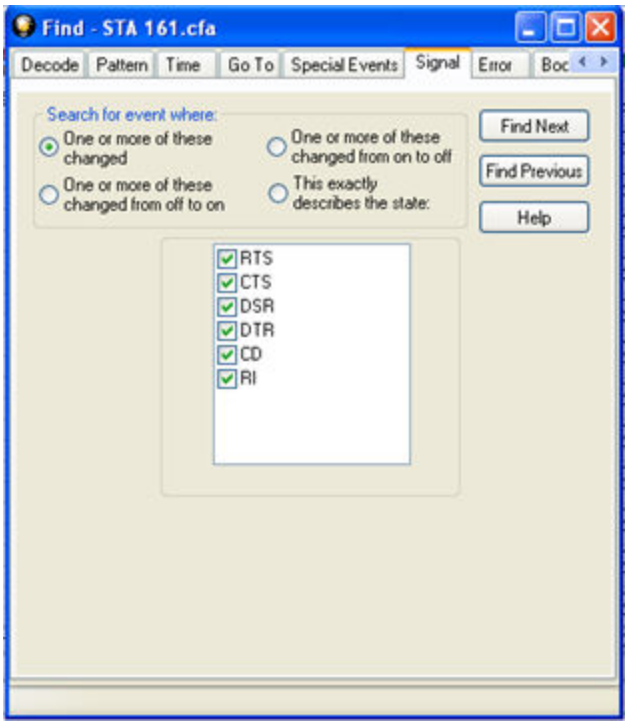


Figure 5.10 - Find Signal Tab

You will choose one qualifier—**Searching for event where**, then choose one or more control signals

Control Signals

The section with the check boxes allows you to specify which control signals the analyzer should pay attention to when doing the search. The analyzer pays attention to any control signal with a check mark.

- Click on a box to place a check mark next to a control signal
- Click again to uncheck the box
- By default, the analyzer searches all control signals, which means all boxes start out checked.

For example, if you are only interested in finding changes in **RTS** and **CTS**, you would check those two boxes and uncheck all the other boxes. This tells the analyzer to look only at the **RTS** and **CTS** lines when running the search. The other signals are ignored.

The control signals types include:

- USB - Pin 1
- USB - Pin 2
- USB - Pin 3
- USB - Pin 4

or

- RS232 - Request to Send (RTS)
- RS232 - Clear to Send (CTS)
- RS232 - Data Set Ready (DSR)
- RS232 - Data Terminal Ready (DTR)
- RS232 - Carrier Detect (CD)
- RS232 - Ring Indicator (RI).

Click here to learn more about the Breakout Box and Pins 1 - 4.

Searching for event where:

- The first three options are all fairly similar, and are described together. These options are searching for an event where:
    - One or more control signals changed
    - One or more control signals changed from off to on
    - One or more control signals changed from on to off
- Searching for an event where one or more signals changed means that the analyzer looks at every control signal that you checked, and see if any one of those signals changed state at any time.

- If you want to look at just one control signal:
  - Check the box for the signal.
  - Uncheck all the other boxes.
  - Choose to search for an event where one or more signals changed.
  - The analyzer notes the state of the selected signal at the point in the buffer where the cursor is, search the buffer, and stop when it finds an event where RTS changed state.
  - If the end of the buffer is reached before an event is found, the analyzer tells you that no matches were found.

- Searching for events where control signals changed state from off to on, or vice versa, is most useful if the signals are usually in one state, and you want to search for occasions where they changed state.

  For example:

  - If DTR is supposed to be on all the time but you suspect that DTR is being dropped
  - Tell the analyzer to look only at DTR by checking the DTR box and unchecking the others
  - Do a search for where one or more control signals changed from on to off.
  - The analyzer would search the DTR signal and stop at the first event where DTR dropped from on to off.

- Searching for an Exact State

  To search for an exact state means that the analyzer finds events that match exactly the state of the control signals that you specify.

  - First, choose to search for an event where your choices exactly describe the state.
  - This changes the normal check boxes to a series of radio buttons labeled On, Off and Don't Care for each control signal.
  - Choose which state you want each control signal to be in.
  - Choose Don't Care to have the analyzer ignore the state of a control signal.
  - When you click Find Next, the analyzer searches for an event that exactly matches the conditions selected, beginning from the currently selected event.
  - If the end of the buffer is reached before a match is found, the analyzer asks you if you want to continue searching from the beginning.
  - If you want to be sure to search the entire buffer, place your cursor on the first event in the buffer.
  - Select one of the four radio buttons to choose the condition that must be met in the search
  - Select one or more of the checkboxes for Pin 1, 2, 3, or 4.
  - Or, **Select one or more of the** checkboxes for Request to Send (**RTS**), Clear to Send (**CTS**), Data Set Ready (**DSR**), Data Terminal Ready (**DTR**), Carrier Detect (**CD**), and Ring Indicator (**RI**).
  - Click **Find Next** to locate the next occurrence of the search criteria or **Find Previous** to locate an earlier occurrence of the search criteria.

5.1.7 Searching for Data Errors

The analyzer can search for several types of data errors. Searching for data error sallows you to choose which errors you want to search for and whether to search the DTE or DCE data or both. Bytes with errors are shown in red in the **Event Display** window, making it easy to find errors visually when looking through the data.

To access the search by time function:

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Errors** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

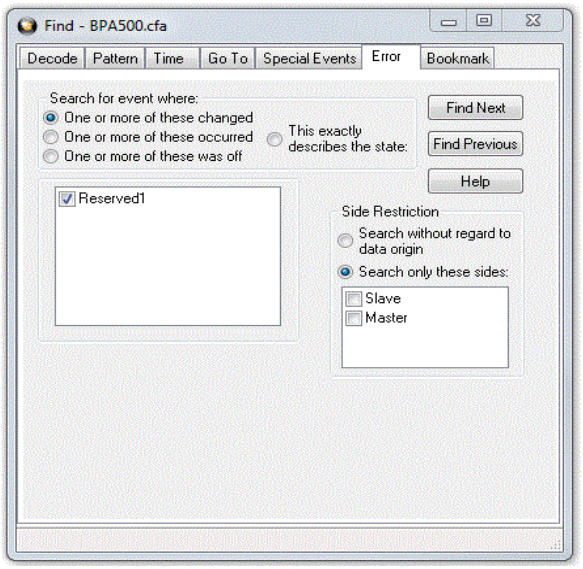


Figure 5.11 - Find Error tab.

Searching for event where

The first three options are all fairly similar, and are described together. These options are searching for an event where:

- one or more error conditions changed
- one or more error conditions occurred
- one or more error conditions were off (i.e. no errors occurred)

Selecting Which Errors to Search

The section with the check boxes allows you to choose which errors the analyzer should look for. Click on a box to check or un-check it.

If you want to search only for overrun errors

- check the box if shown
- un-check the other boxes.

To search for all types of errors

- check all boxes

The most common search is looking for a few scattered errors in otherwise clean data.

To do this type of search:

- choose to **Search for an event where** one or more error conditions occurred
- choose which errors to look for
- By default, the analyzer looks for all types of errors.

In contrast, searching for an event where one or more error conditions were off means that the analyzer looks for an event where the errors were not present.

For example, if you have data that is full of framing errors, and you know that somewhere in your 20 megabyte capture file the framing got straightened out, you could choose to search for an event where one or more error conditions were off, and choose to search only for framing. The analyzer searches the file, and finds the point at which framing errors stopped occurring.

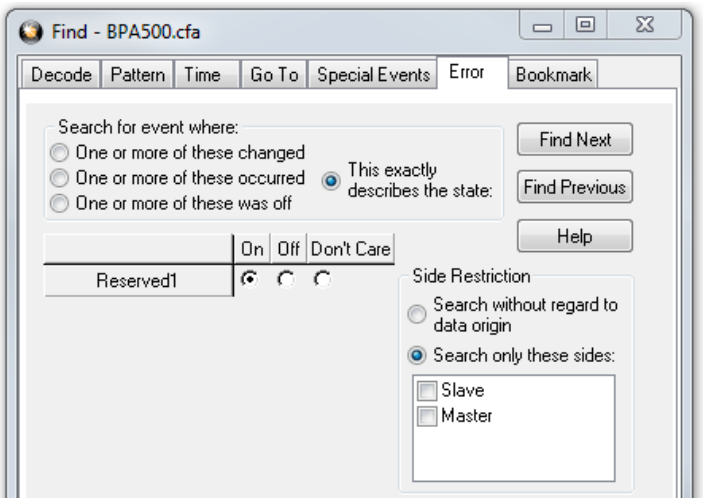
Searching for an event where the error conditions changed means that the analyzer searches the data and stop at every point where the error condition changed from on to off, or off to on.

For example, if you have data where sometimes the framing is wrong and sometimes right, you would choose to search framing errors where the error condition changed. This first takes you to the point where the framing errors stopped occurring. When you click **Find Next,** the analyzer stops at the point when the errors began occurring again. Clicking **Find Previous** will search backwards from the current postion.

The analyzer takes the current selected byte as its initial condition when running searches that rely on finding events where error conditions changed. The analyzer searches until it finds an event where error conditions changed or it reaches the end of the buffer, at which point the analyzer tells you that there are no more events found in the buffer. If you are searching for an exact match, the analyzer asks you if you want to continue searching from the beginning of the buffer.

Searching for Exact Error Conditions

To search for an exact state means that the analyzer finds events that exactly match the error conditions that you specify.



- Select the **This exactly describes the state** radio button.
- This changes the normal check boxes to a series of radio buttons labeled **On**, **Off** and **Don't Care** for each error.
  - **On** means that the error occurred
  - **Off** means that the error did not occur
  - **Don't Care** means that the analyzer ignores that error condition.
- Select the appropriate state for each type of error.

Example:

If you need to find an event where just an overrun error occurred, but not any other type of error, you would choose overrun error to be On, and set all other errors to Off. This causes the analyzer to look for an event where only an overrun error occurred.

If you want to look for events where overrun errors occurred, and other errors may have also occurred but it really doesn't matter if they did or not, choose overrun to be On, and set the others to Don't Care. The analyzer ignores any other type of error, and find events where overrun errors occurred.

To find the next error, click the Find Next button. To find an error that occurred earlier in the buffer to where you are, click the Find Previous button.

5.1.8 Find - Bookmarks

Searching with **Bookmarks** allows you search on specific bookmarks on the data in **Frame Display** and **Event Display** window. Bookmarks are notes/reminders of interest that you attach to the data so they can be accessed later.

To access the search for bookmarks

1. Open a capture file to search.
2. Open the **Event Display** or **Frame Display** window.
3. Click on the **Find** icon or choose **Find** from the **Edit** menu.
4. Click on the **Bookmarks** tab of the **Find** dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

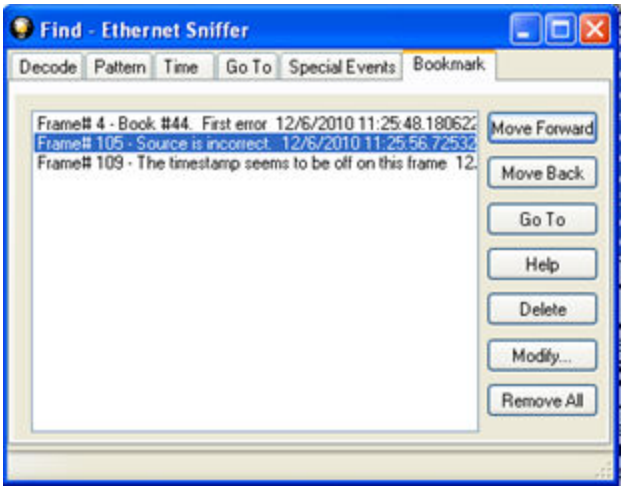


Figure 5.12 - Find Bookmark tab.

There are several ways to locate bookmarks.

- Select the bookmark you want to move to and click the **Go To** button.
- Simply double-click on the bookmark.
- Click the **Move Forward** and **Move Back** buttons to move through the frames to the bookmarks shown in the window. When the bookmark is found it is highlighted in the window.

There are three ways to modify bookmarks:

1. Click on **Delete** to remove the selected bookmark.
2. Click on **Modify...** to change the selected Bookmark name.
3. **Remove All** will delete all bookmarks in the window.

The **Find** window **Bookmark** tab will also appear when using functions other than **Find** such as when clicking on the Display All Bookmarks icon.

5.1.9 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the **Event Display**. The first selected byte appears on the third line of the display.

```
[CVEventDisplay]
SelectionOffset=2
```

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\User\Public\Public Documents\Frontline Test Equipment\)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

5.1.10 Subtleties of Timestamp Searching

Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

5.2 Bookmarks

Bookmarks are electronic sticky notes that you attach to frames of interest so they can be easily found later. In **Frame Display** bookmarked frames appear with a magenta triangle icon next to them.

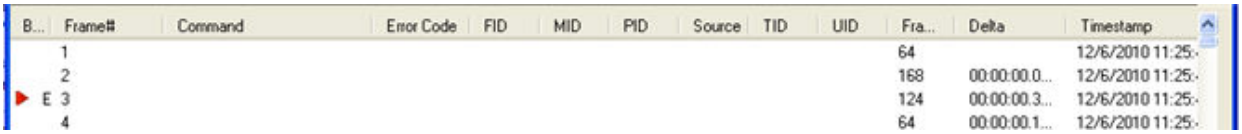
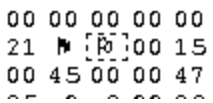


Figure 5.13 - Bookmarked Frame (3) in the Frame Display



In the **Event Display** bookmarks appear as a dashed line around the start of frame marker.

Bookmarks are easy to create and maintain, and are a very valuable tool for data analysis. When you create or modify a bookmark, you have up to 84 characters to explain a problem, leave yourself a reminder, leave someone else a reminder, etc. Once you create a bookmark it will be saved with the rest of the data in the .cfa file. When you open a .cfa file, the bookmarks are available to you.

Once you have created a bookmark, you can use the Find function or other navigation methods to locate and move among them.

5.2.1 Adding, Modifying or Deleting a Bookmark

You can add, modify, or delete a bookmarks from **Frame Display** and **Event Display**

Add:

1. Select the frame or event you want to bookmark.
2. There are three ways to access the **Add Bookmark** dialog.
    a. Select **Add or Modify Bookmark** from the **Bookmarks** menu on the **Frame Display** and **Event Display**,
    b. Select the **Add or Modify Bookmark** icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing **Add Bookmark...**.
3. In the dialog box, add a comment (up to 84 characters) in the text box to identify the bookmark.
4. Click **OK**.

Once you create a bookmark it will be saved with the rest of the data in the .cfa file. When you open a .cfa file, the bookmarks are available to you.

Modify

1. Select the frame or event with the bookmark to be edited.
2. There are three ways to access the **Add/Modfy Bookmark** dialog.
    a. Select **Add or Modify Bookmark** from the **Bookmarks** menu on the **Frame Display** and **Event Display**'
    b. Select the **Add or Modify Bookmark** icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing **Modify Bookmark...** on the selection.
3. Change the comment in the dialog box
4. Click **OK**. The edited bookmark will be saved as a part of the .cfa file.
5. You can also select **Display All Bookmarks** from the **Frame Display** and **Event Display** toolbar or the **Bookmarks** menu. the **Find** window will open on the **Bookmark** tab. Select the bookmark you want to modify and click the **Modify...** button. Change the comment in the dialog box, and click **OK**.

Delete

1. Select the frame or event with the bookmark to be deleted.
2. There are three ways to access the **Add/Modfy Bookmark** dialog.
    a. Select **Add or Modify Bookmark** from the **Bookmarks** menu on the **Frame Display** and **Event Display**,
    b. Select the **Add or Modify Bookmark** icon on one of the toolbars, or
    c. Right-click on the frame/event and choosing **Modify Bookmark...** on the selection.
3. Click on the **Delete** button. The bookmark will be deleted.
4. You can also select **Display All Bookmarks** from the **Frame Display** and **Event Display** toolbar or the **Bookmarks** menu. the **Find** window will open on the **Bookmark** tab. Select the bookmark you want to delete and click the **Delete** button.

5.2.2 Displaying All and Moving Between Bookmarks

There are three ways to move between bookmarks.

1. Press the F2 key to move to the next frame or event with a bookmark.
2. Select Go to Next Bookmark from the Bookmarks menu.
3. Click the Display All Bookmarks icon . Select the bookmark you want to move to and click the Go To button, or simply double-click on the bookmark. Click the Move Forward and Move Back buttons to cycle through the bookmarks.

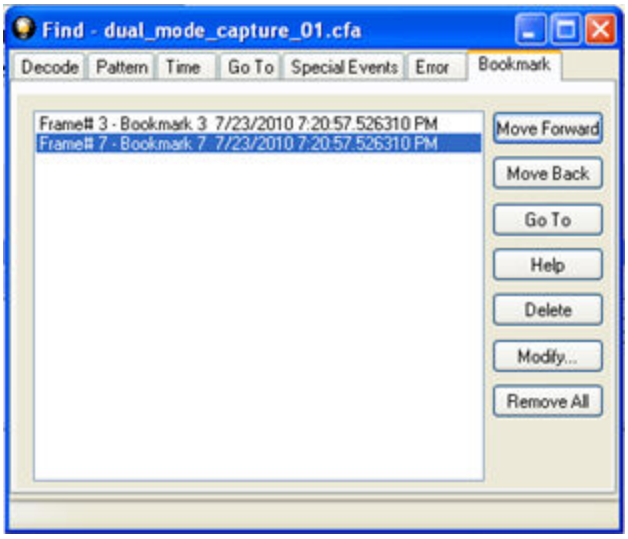


Figure 5.14 - Find Window Bookmark tab Used to Move Around With Bookmarks

To delete a bookmark, select it and click the **Delete** button.

To modify a bookmark, select it and click the **Modify** button.

Click **Remove All** to delete all the bookmarks.

Chapter 6 Saving and Importing Data

6.1 Saving Your Data

You can save all or part of the data that you have captured. You can also load a previously saved capture file, and save a portion of that file to another file. This feature is useful if someone else needs to see only a portion of the data in your capture file.

On the **Control** window toolbar you can set up to capture a single file. Click here to see those settings.

There are two ways to save portions or all of the data collected during a data capture. Click here to see how to capture data to disk.

6.1.1 Saving the Entire Capture File

This option is only available when you select **Single File** from the **Capture Mode** on **System Settings.** Click here to learn more about selecting Save options from System Settings.

1. If you are capturing data, click on the **Stop Capture** icon to stop data capture. You cannot save data to file while it is being captured.
2. Open the **Event Display** or **Frame Display** window.
3. Click the **Save** icon, or select **Save** from the **File** menu.

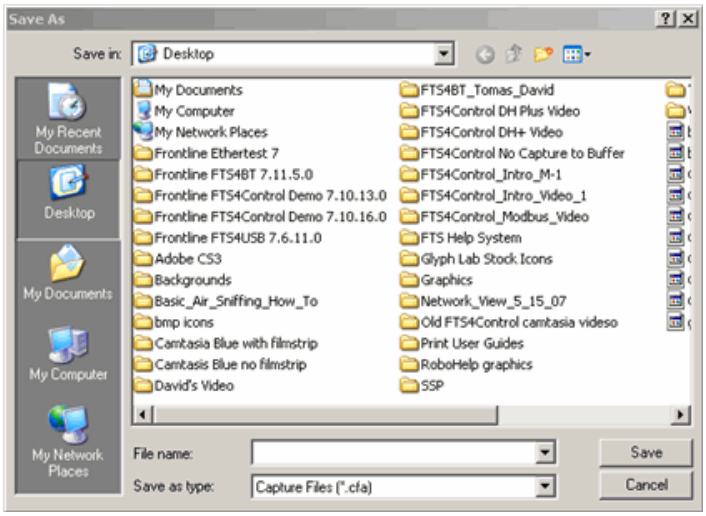
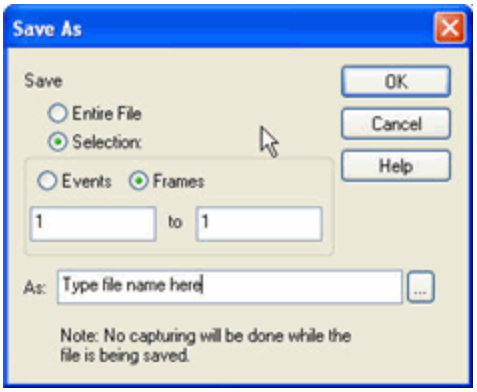


Figure 6.1 - Windows Save dialog

4. Type a file name in the **File name** box at the bottom of the screen.
5. Browse to select a specific directory. Otherwise your file is saved in the default capture file directory.
6. When you are finished, click **OK**.

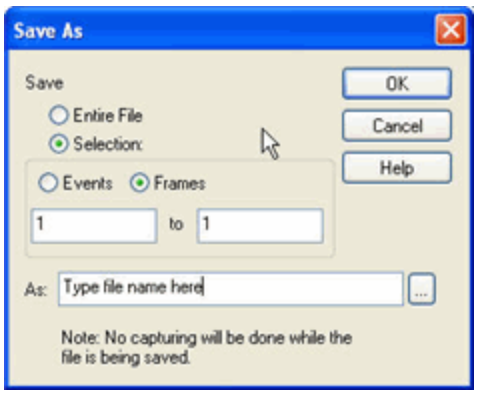
6.1.2 Saving the Entire Capture File with Save Selection

1. If you are capturing data, click on the **Stop** icon to stop data capture. You cannot save data to file while it is being captured.
2. Open the **Event Display** or **Frame Display** window.
3. Right click in the data
4. Select **Save Selection** or **Save As** from the right click menu.
5. Click on the radio button labeled **Entire File**.
6. Choose to save **Events** or **Frames** . Choosing to save **Events** saves the entire contents of the capture file. Choosing to save **Frames** does not save all events in the capture file.
7. Type a file name in the **As** box at the bottom of the screen. Click the **Browse** icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
8. When you are finished, click **OK**.



6.1.3 Saving a Portion of a Capture File

1. If you are capturing data, click on the **Stop** icon to pause data capture. You cannot save data to a file while it is being captured.
2. Open the **Event Display** or **Frame Display** window, depending on whether you want to specify a range in bytes or in frames.
3. Select the portion of the data that you want to save. Click and drag to select data, or click on the first item, move to the last item and Shift+Click to select the entire range, or use the Shift key with the keyboard arrows or the navigation icons in the **Frame Display** toolbar. If the range you want to save is too large to select, note the numbers of the first and last item in the range.
4. Right click in the data
5. Select **Save Selection** or **Save As** from the right click menu
6. Click on the radio button labeled **Selection**. If you selected a range, make sure the starting and ending numbers are correct. To specify a range, type the numbers of the first and last items in the range in the boxes.
7. Select either **Events** or **Frames** to indicate whether the numbers are event or frame numbers.
8. Type a file name in the **As** box at the bottom of the screen. Click the **Browse** icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
9. Click **OK** when you are finished.



6.2 Adding Comments to a Capture File

The **Notes** feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the **Notes** window :

1. Click the **Show Notes** icon . This icon is present on the toolbars of the **Frame Display** , as well as the **Event Display** . **Notes** can be selected from the **Edit** menu on one of these windows.

2. Type your comments in the large edit box on the **Notes** window. The **Cut**, **Copy**, **Paste** features are supported from **Edit** menu and the toolbar when text is selected. Undo and Redo features are all supported from **Edit** menu and the toolbar at the current cursor location.
3. Click the thumbtack icon to keep the **Notes** window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

6.3 Confirm Capture File (CFA) Changes

This dialog appears when you close a capture file after changing the Notes, the protocol stack, or bookmarks. The dialog lists information that was added or changed and allows you to select which information to save, and whether to save it to the current file or to a new one.

Changes made to the file appear in a list in the left pane. You can click on each item to see details in the right pane about what was changed for each item. You simply check the boxes next to the changes you want to keep. Once you decide what changes to keep, select one of the following:

- **Save To This File** – Saves the changes you have made to the current capture file.
- **Save As** – Saves the changes to a new file.
- **Cancel the Close Operation** – Closes the file and returns you back to the display. No changes are saved.
- **Discard Changes** – Closes the file without saving any of the changes made to the notes, bookmarks, or protocol stack.

6.4 Loading and Importing a Capture File

6.4.1 Loading a Capture File

From the Control Window:

1. Go to the **File** menu.
2. Choose a file from the recently used file list.
3. If the file is not in the **File** menu list, select **Open Capture File** from the **File** menu or simply click on the **Open** icon on the toolbar.
4. Capture files have a .cfa extension. Browse if necessary to find your capture file.
5. Click on your file, and then click **Open**.

6.4.2 Importing Capture Files

1. From the **Control** window , go to the **File** menu and select Open Capture File or click on the Open icon on the toolbar.
2. Left of the **File name** text box, select from the drop-down list **Supported File Types** box to All Importable File Types or **All Supported File Types (*.cfa, *.log, *.txt, *.csv, *.cap)**. Select the file and click **Open**.

The analyzer automatically converts the file to the analyzer's format while keeping the original file in its original format. You can save the file in the analyzer's format, close the file without saving it in the analyzer's format, or have the analyzer automatically save the file in the analyzer's format (see the System Settings to set this option). All of these options keep your original file untouched.

When you first open the file, the analyzer brings up the Protocol Stack window and ask you what protocol decodes, if any, you want to use. You must choose a protocol decode at this point for the analyzer to decode the data in the file. If you open a file without using any decodes, and decide later that you want to apply a decode, choose Reframe from the File menu on the Control window.

At present, the analyzer supports the following file types:

- Frontline Serialtest* Async and Serialtest ComProbe® for DOS – requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- Greenleaf ViewComm* 3.0 for DOS - requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- Frontline Ethertest* for DOS – requires 3 files: filename.cap, filename.ca0 and filename.ca1.
- Sniffer Type 1 – supports files with the .enc extension. Does not support Sniffer files with a .cap extension.
- Snoop or Sun Snoop – files with a .cap extension based on RFC 1761. For file format, see http://www.faqs.org/rfcs/rfc1761.html.
- Shomiti Surveyor files in Snoop format – files with a .cap extension. For file format, contact Technical Support.
- CATC Merlin - files with a .csv extension. Files must be exported with a specific format. See File Format for Merlin Files for information.
- CATC Chief - files with a .txt extension.

6.5 Printing

6.5.1 Printing from the Frame Display/HTML Export

The **Frame Display Print** dialog and the **Frame Display HTML Export** are very similar. This topic discusses both dialogs.

Frame Display Print

The **Frame Display Print** feature provides the user with the option to print the capture buffer or the current selection. The maximum file size, however, that can be exported is 1000 frames.

When **Print Preview** is selected, the output displays in a browser print preview window, where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images.

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select “Internet Options…” menu entry.
3. Click Advanced tab.
4. Check “Print background colors and images” under the Printing section
5. Click the Apply button, then click OK

Configure the Print File Range in the Frame Display Print Dialog

Selecting more than one frame in the Frame Display window defaults the radio button in the Frame Display Print dialog to Selection and allows the user to choose the All radio button. When only one frame is selected, the All radio button in the Frame Display Print dialog is selected.

How to Print Frame Display Data

1. Select **Print** or **Print Preview** from the **File** menu on the **Frame Display** window to display the **Frame Display Print** dialog. Select **Print** if you just want to print your data to your default printer. Select **Print Preview** if you want access to printer options.
2. Choose to include the **Summary** pane (check the box) in the print output. The **Summary** pane appears at the beginning of the printed output in tabular format. If you select **All layers** in the **Detail Section**, the **Data Bytes** option becomes available.
3. In the **Detail Section**, choose to exclude—**No decode section**—the decode from the **Detail** pane in the **Frame Display**, or include **All Layers** or **Selected Layers Only.** If you choose to include selected layers, then select (click on and highlight) the layers from the list box.
4. Click on selected layers in the list to de-select, or click the **Reset Selected Layers** button to de-select all selected layers.

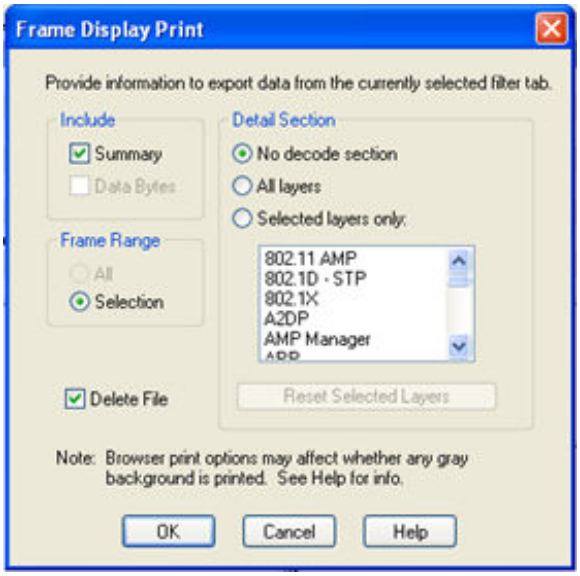


Figure 6.2 - Frame Display Print Dialog

5. Select the range of frames to include **All** or **Selection** in the **Frame Range** section of the **Frame Display Print** dialog.

   Choosing **All** prints up to 1000 frames from the buffer.

   Choosing **Selection** prints only the frames you select in the Frame Display window.

6. Selecting the **Delete File** deletes the temporary html file that was used during printing
7. Click the **OK** button.

Frame Display Print Preview

The **Frame Display Print Preview** feature provides the user with the option to export the capture buffer to an .html file. The maximum file size, however, that can be exported is 1000 frames.

If you chose **Print Preview**, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

1. Select **Print Preview** from the **File** menu on the **Frame Display** window to display the **Frame Display Print Preview**.

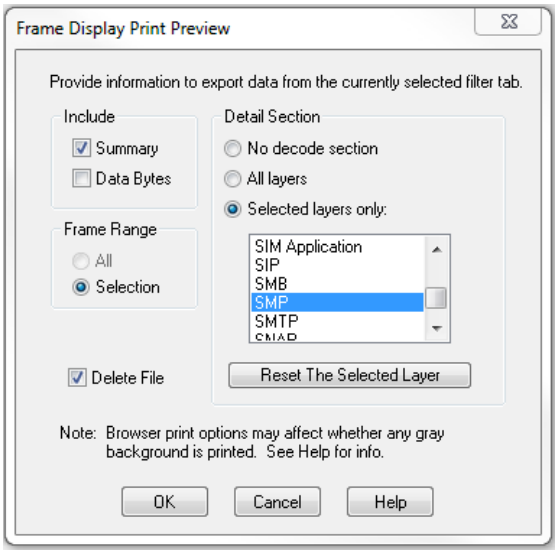


Figure 6.3 - Frame Display Print Preview Dialog

2. From this point the procedure is the same as steps 2 through 5 in "How to Print Frame Display Data" above.
3. Click the **OK** button, and after a brief wait a browser window will appear.

6.5.2 Printing from the Event Display

The Event Display Print feature provides the user with the option to print either the entire capture buffer or the current selection. When Print Preview is selected, the output displays in a browser print preview window where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select “Internet Options…” menu entry.
3. Click Advanced tab.
4. Check “Print background colors and images” under the Printing section
5. Click the Apply button, then click OK

The **Event Display Print** feature uses the current format of the **Event Display** as specified by the user.

See About Event Display for an explanation on formatting the **Event Display** prior to initiating the print feature.

Configure the Print File Range in the Event Display Print dialog

Selecting more than one event in the **Event Display** window defaults the radio button in the **Event Display Print** dialog to **Selection** and allows the user to choose the **All** radio button. When only one event is selected , the **All** radio button in the **Event Display Print** dialog is selected.

How to Print Event Display Data to a Browser

1. Select **Print** or **Print Preview** from the **File** menu on the **Event Display** window to display the **Event Display Print** dialog. Select **Print** if you just want to print your data to your default printer. Select **Print Preview** if you want preview the print in your browser.
2. Select the range of events to include from either **All** or **Selection** in the **Event Range** section . Choosing **All** prints all of the events in the capture file or buffer. Choosing **Selection** prints only the selected events in the Event Display window.

Note: In order to prevent a Print crash, you cannot select **All** if there are more than 100,000 events in the capture buffer.

Note: See "Configure the Print File Range in the Event Display Print Dialog" above for an explanation of these selections

Figure 6.4 - Event Display Print Dialog

3. Click the OK button.

If you chose **Print Preview**, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

6.6 Exporting

6.6.1 Frame Display Export

You can dump the contents of the **Summary** pane on the **Frame Display** into a Comma Separated File (.csv).

To access this feature:

1. Right click on the **Summary** pane or open the **Frame Display File** menu.
2. Select the **Export...** menu item.
3. Select a storage location and enter a **File name**.
4. Select **Save**.

6.6.2 Exporting a File with Event Display Export

With the **Event Display Export** dialog you can export the contents of the **Event Display** dialog as a test (.txt), CSV (.csv.), HTML (.htm), or Binary File (.bin). You also have the option of exporting the entire capture buffer or just the current selection of the Event Display dialog.

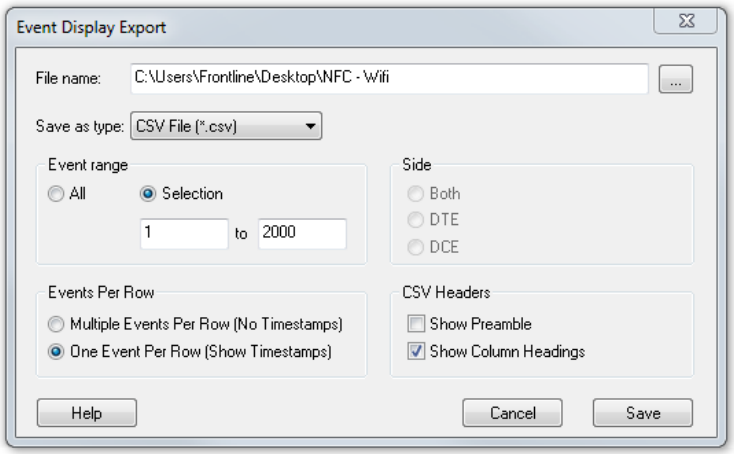


Figure 6.5 - Event Display Export Example: .csv file.

How to Export Event Display Data to a File

1. Select **Export Events** from the **File** menu on the **Event Display** window to display the **Event Display Export** dialog.
2. Enter a file path and name, or click the browser button to display the Windows **Save As** dialog and navigate to the desired storage location.
3. Select a file type from the **Save as type:** drop-down List Menu on the Event Display Export dialog. Select from among the following file formats:

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

   Binary File (*.bin)
4. Select the range of events to include in the file from either **All** or **Selection** in the **Event Range** section of the **Event Display Export** dialog.
   - Selecting more than one event in the Event Display window defaults the radio button in the Event Display Export dialog to Selection and allows the user to choose the All radio button.
   - When only one event is selected (something must be selected), the All radio button in the Event Display Export dialog is selected by default.
5. Next you need to select the Side variable for serial communications.
   - is used to determine whether you want to export data from , or both.
   - Choose Host, Function\Control or Both to determine how you want to export the data.
5. Choose Host, Function\Control or Both to determine how you want to export the data.
6. Choose whether you want to display multiple events or single events per row.

Events Per Row: You can choose to display **Multiple Events Per Row**, but this method contains no timestamps. If you select **One Event Per Row**, you can display timestamps. multiple events or single events per row.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

.

The timestamp data types displayed in columns for One Event Per Row.

Timestamp

Delta

Event Number

Byte Number

Frame Number

Type

Hex

Dec

Oct

Bin

Side

ASCII | 7-bit ASCII | EBCDIC | Baudot

RTS

CTS

DSR

DTR

CD

RI

UART Overrun

Parity Error

Framing Error

7. If you select .csv as the file type, choose whether you want to hide/display **Preambles** or **Column Headings** in the exported file
8. Click **Save**. The Event Display Export file is saved to the locations you specified in **File name**.

	A	B	C	D	E	F	G	H	I	J	K
1	Timestamp	Delta	Event Number	Byte Number	Frame Number	Type	Hex	Dec	Oct	Bin	ASCII
632	11/30/2012 12:20:02.895166 PM	0:00:00.00	631	626	3	Data	0	0	0	0	.
633	11/30/2012 12:20:02.895166 PM	0:00:00.00	632	627	3	Data	0	0	0	0	.
634	11/30/2012 12:20:02.895166 PM	0:00:00.00	633	628	3	Data	0	0	0	0	.
635	11/30/2012 12:20:02.895166 PM	0:00:00.00	634	629	3	Data	98	152	230	10011000	.
636	11/30/2012 12:20:02.895166 PM	0:00:00.00	635	630	3	Data	70	112	160	1110000	p
637	11/30/2012 12:20:02.895166 PM	0:00:00.00	636	631	3	Data	94	148	224	10010100	.
638	11/30/2012 12:20:02.895166 PM	0:00:00.00	637	632	3	Data	22	34	42	100010	"
639	11/30/2012 12:20:02.895166 PM	0:00:00.00	638	633	3	Data	21	33	41	100001	!
640	11/30/2012 12:20:02.895166 PM	0:00:00.00	639	634	3	Data	1c	28	34	11100	.
641	11/30/2012 12:20:02.895166 PM	0:00:00.00	640	635	3	Data	80	128	200	10000000	.
642	11/30/2012 12:20:02.895166 PM	0:00:00.00	641	636	3	Data	80	128	200	10000000	.
643	11/30/2012 12:20:02.895166 PM	0:00:00.00	642	637	3	Data	80	128	200	10000000	.
644	11/30/2012 12:20:02.895166 PM	0:00:00.00	643	638	3	Data	80	128	200	10000000	.

Figure 6.6 - Example: .csv Event Display Export, Excel spreadsheet

6.6.2.1 Export Filter Out

You can filter out data you don't want or need in your text file.

(This option is available only for serial data.) In the **Filter Out** box, choose which side to filter out: the DTE data, the DCE data or neither side (don't filter any data.) For example, if you choose the radio button for DTE data, the DTE data would be filtered out of your export file and the file would contain only the DCE data.

You can also filter out Special Events (which is everything that is not a data byte, such as control signal changes and Set I/O events), Non-printable characters or both. If you choose to filter out Special Events, your export file would contain only the data bytes. Filtering out the non-printable characters means that your export file would contain only special events and data bytes classified as printable. In ASCII, printable characters are those with hex values between $20 and $7e.

6.6.2.2 Exporting Baudot

When exporting Baudot, you need to be able to determine the state of the shift character. In a text export, the state of the shift bit can be determined by the data in the Character field. When letters is active, the character field shows letters and vice versa.

Chapter 7 General Information

7.1 System Settings and Progam Options

7.1.1 System Settings

Open the **System Settings** window by choosing **System Settings** from the **Options** menu on the **Control** window. To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.

Single File

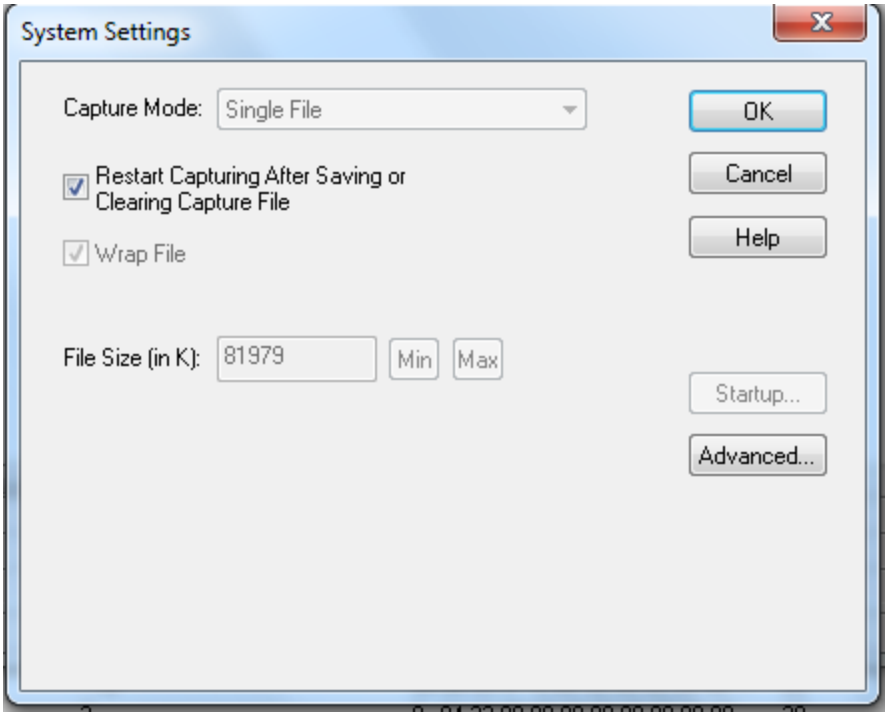


Figure 7.1 - System Settings Single File Mode

This option allows the analyzer to capture data to a file. Each time you capture the file you must provide a file name. The size of each file cannot larger than the number given in File Size (in K). The name of each file is the name you give it in the Name box followed by the date and time. The date and time are when the series was opened.

- **Restart Capturing After Saving or Clearing Capture File**

  If the Automatically Restart feature is enabled, the analyzer restarts capture to the file immediately after the file is closed.

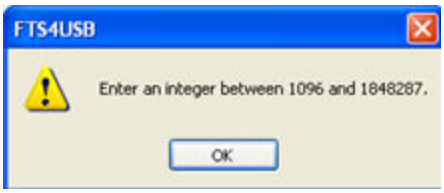
- **Wrap File**

  When enabled, the analyzer wraps the file when it becomes full. The oldest events are moved out of the file to make room for new events. Any events moved out of the file are lost. When disabled, the analyzer stops capture when the file becomes full. Either reset the file or close your capture file to continue.

- **File Size**: The size of the file will depend of the available hard disk space.

  1. Click the **Min** button to see/set the minimum acceptable value for the file size.

  2. Click the **Max** button to see/set the maximum acceptable value for the file size.



You can accept these values, or you can enter a unique file size. But if you try to close the dialog after entering a value greater than the maximum or less than the minimum, you will see the following dialog.

- **Start up**

  Opens the Program Start up Options window. **Start up** options let you choose whether to start data capture immediately on opening the analyzer.

- **Advanced**

  Opens the Advanced System Options window. The Advanced Settings should only be changed on advice of technical support.

7.1.1.1 System Settings - Disabled/Enabled Options

Some of the **System Settings** options are disabled depending upon the status of the data capture session.

- As the default, all the options on the **System Settings** dialog are enabled.
- Once the user begins to capture data by selecting the Start Capture button, some of the options on the System Settings dialog are disabled until the user stops data capture and either saves or erases the captured data.
- The user can go into the **Startup** options and **Advanced** system options on the **System Settings** dialog and make changes to the settings at any time.

7.1.1.2 Advanced System Options

These parameters affect fundamental aspects of the software, and it is unlikely that you ever have to change them. If you do change them and need to return them to their original values, the default value is listed in parentheses to the right of the value box.

Most technical support problems are not related to these parameters, and as changing them could have serious consequences for the performance of the analyzer, we strongly recommend contacting technical support before changing any of these parameters.

To access the Advanced System Options:

1. Go to the Control window.
2. Choose **System Settings** from the **Options** menu.
3. On the **System Settings** window, click the **Advanced** button.

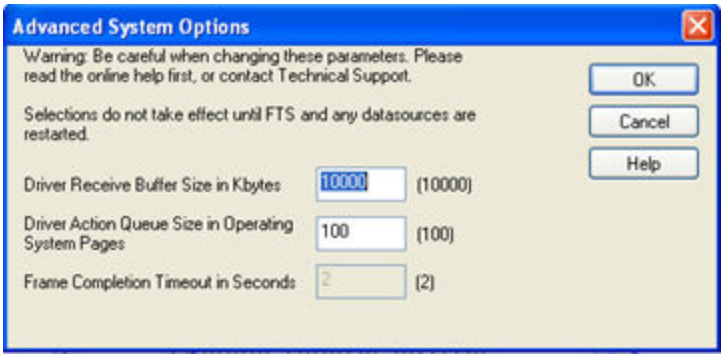

Advanced System Options
Warning: Be careful when changing these parameters. Please read the online help first, or contact Technical Support.
Selections do not take effect until FTS and any datasources are restarted.
OK
Cancel
Help
Driver Receive Buffer Size in Kbytes
10000
(10000)
Driver Action Queue Size in Operating System Pages
100
(100)
Frame Completion Timeout in Seconds
2
(2)

Figure 7.2 - Advanced System Options dialog

- **Driver Receive Buffer Size in Kbytes** - This is the size of the buffer used by the driver to store incoming data. This value is expressed in Kbytes.
- **Driver Action Queue Size In Operating System Pages** - This is the size of the buffer used by the driver to store data to be transmitted. This value is expressed in operating system pages.
- **Frame Completion Timeout in Seconds** - This is the number of seconds that the analyzer waits to receive data on a side while in the midst of receiving a frame on that side.

  If no data comes in on that side for longer than the specified number of seconds, an "aborted frame" event is added to the Event Display and the analyzer resumes decoding incoming data. This can occur when capturing interwoven data (DTE and DCE) and one side stops transmitting in the middle of a frame.

  The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

Note: This option is currently disabled.

7.1.1.3 Selecting Start Up Options

To open this window:

1. Choose **System Settings** from the **Options** menu on the Control window.
2. On the System Settings window, click the **Start Up** button.
3. Choose one of the options to determine if the analyzer starts data capture immediately on starting up or not.

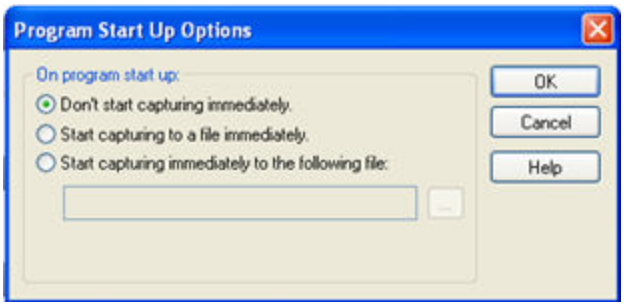


Figure 7.3 - Start Up Options dialog

- **Don't start capturing immediately** - This is the default setting. The analyzer begins monitoring data but does not begin capturing data until clicking the **Start Capture** icon on the **Control**, **Event Display** or **Frame Display** windows.
- **Start capturing to a file immediately** - When the analyzer starts up, it immediately opens a capture file and begins data capture to it. This is the equivalent of clicking the**Start Capture** icon. The file is given a name based on the settings for capturing to a file or series of files in the **System Settings** window.
- **Start capturing immediately to the following file:** - Enter a file name in the box below this option. When the analyzer starts up, it immediately begins data capture to that file. If the file already exists, the data in it is overwritten.

7.1.2 Changing Default File Locations

The analyzer saves user files in specific locations by default. Capture files are placed in the My Capture Files directory and configurations are put in My Configurations. These locations are set at installation.

Follow the steps below to change the default locations.

1. Choose **Directories** from the **Options** menu on the **Control** window to open the **File Locations** window.

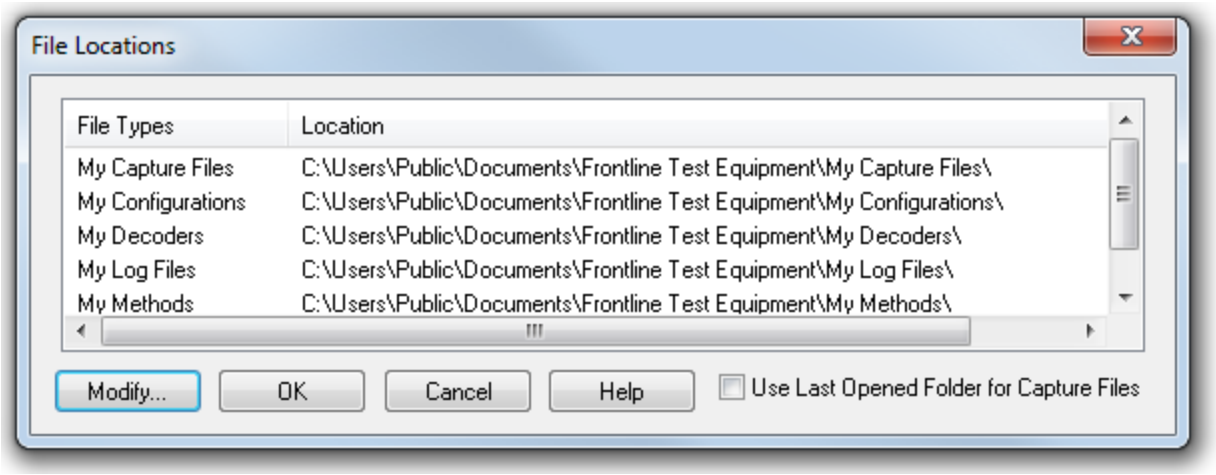


Figure 7.4 - File Locations dialog

2. Select the default location you wish to change.
3. Click **Modify**.
4. Browse to a new location.

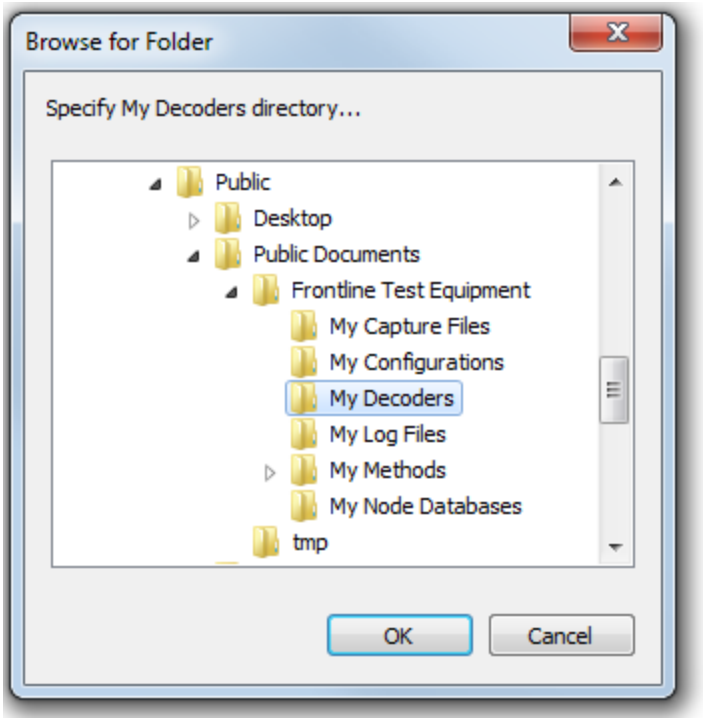


Figure 7.5 - File Locations Browse dialog

5. Click **OK**.
6. Click **OK** when finished.

If a user sets the My Decoders directory such that it is up-directory from an installation path, multiple instances of a personality entry may be detected, which causes a failure when trying to launch Frontline. For example, if an Frontline product is installed at C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\ then "My Decoders" cannot be set to any of the following:

- C:\ My Decoders\
- C:\Users\ My Decoders\
- C:\Users\\Public\My Decoders\
- C:\Users\Public\Public Documents\My Decoders\
- or to any directory that already exists in the path C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\

Default Capture File Folder Checkbox

If the **Use Last Opened Folder for Capture Files** checkbox is checked, then the system automatically changes the default location for saving capture files each time you open a file from or save a file to a new location. For example, let's say the default location for saving capture files is Drive A > Folder A. Now you select the **Use Last Opened Folder for Capture Files** checkbox. The next time, however, you open a capture file from a different location, Folder B > Removable Flash Drive for example. Now when you save the capture file, it will be saved to Folder B > Removable Flash Drive. Also, all subsequent files will be saved to that location. This remains true until you open a file from or save a file to a different location.

There is one caveat to this scenario, however. Let's say you have selected **Use Last Opened Folder for Capture Files** and opened a file from a location other than the default directory. All subsequent capture files will be saved to that location. Suppose, however, the next time you want to save a capture file, the new file location is not available because the directory structure has changed: a folder has been moved, a drive has been reassigned, a flash drive has been disconnected, etc. In the case of a "lost" directory structure, subsequent capture files will be saved to the default location. **ComProbe software will always try to save a file to the folder where the last file was opened from or saved to, if Use Last Opened Folder for Capture Files is checked.** If, however, the location is not accessible, files are saved to the default directory that is set at installation.

If the checkbox is unchecked, then the system always defaults to the directory listed in the File Locations dialog.

7.1.3 Side Names

The **Side Names** dialog is used to change the names of objects and events that appear in various displays. **The Side Names** dialog will change depending on the sniffing technology in use at the time the software was loaded.

Changes to the Names are used throughout the program.

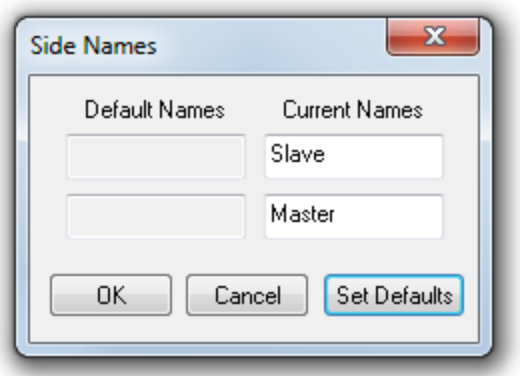


Figure 7.6 - Example: Side Names Where "Slave" and "Master" are current

1. To open the Side Names dialog, choose **Side Names...** from the **Options** menu on the **Control** window.
2. To change a name, click on the name given in the **Current Names** column, and then click again to modify the name (a slow double-click).
3. Select **OK** to initiate the changes. The changes that have been made will not fully take effect for any views already open. Closing and reopening the views will cause the name change to take effect.
4. To restore the default values, click the **Set Defaults** button.

7.1.4 Timestamping

Timestamping is the process of precise recording in time of packet arrival. Timestamps is an optional parameter in the Frame Display and Event Display that can assist in troubleshooting a network link.

7.1.4.1 Timestamping Options

The Timestamping Options window allows you to enable or disable timestamping, and change the resolution of the timestamps for both capture and display purposes.

To open this window:

Choose **Set Timestamp Format...** from the **Options** menu on the Frame Display and Event Display window or click on the **Timestamping Option** icon in the **Event Display** toolbar. The Timestamping Options window will open.

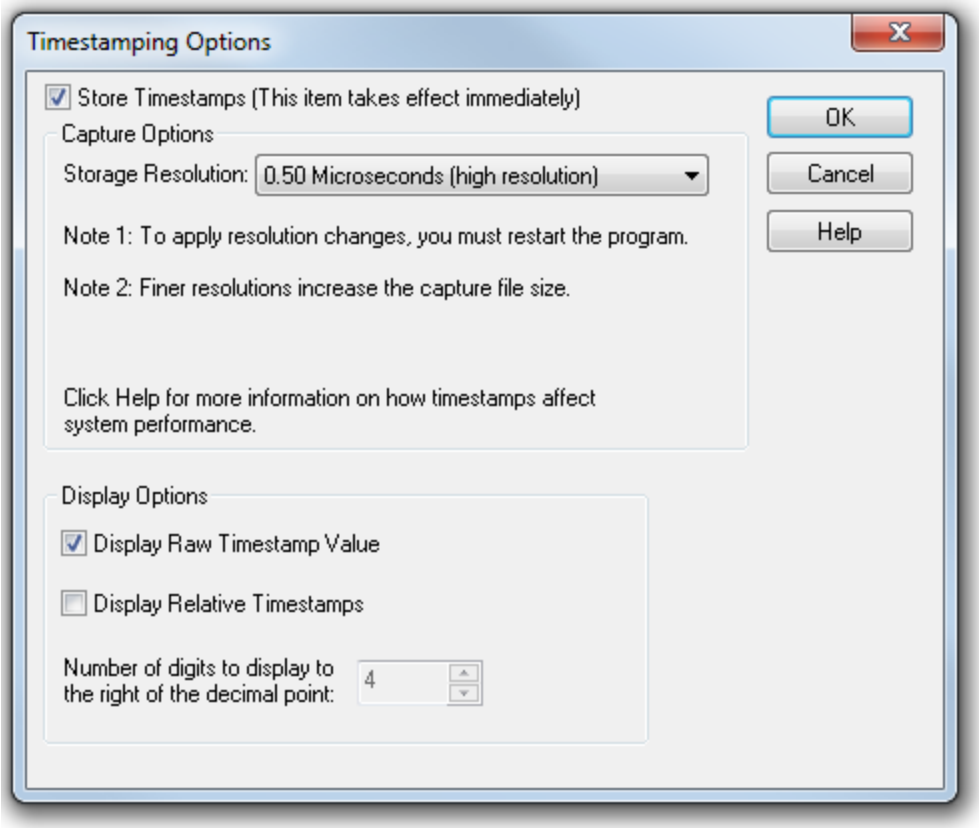

Timestamping Options
Store Timestamps (This item takes effect immediately)
Capture Options
Storage Resolution: 0.50 Microseconds (high resolution)
Note 1: To apply resolution changes, you must restart the program.
Note 2: Finer resolutions increase the capture file size.
Click Help for more information on how timestamps affect system performance.
Display Options
Display Raw Timestamp Value
Display Relative Timestamps
Number of digits to display to the right of the decimal point: 4
OK
Cancel
Help

Figure 7.1 Timestamping Options dialog

7.1.4.2 Enabling/Disabling Timestamp

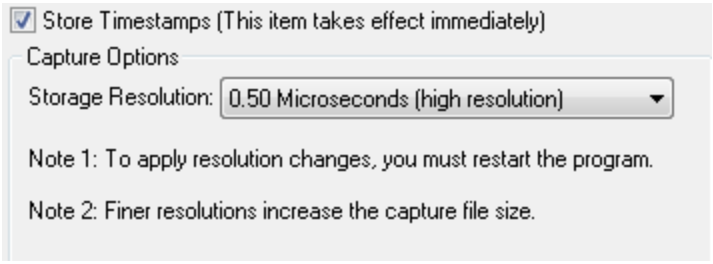
To enable timestamping click to make a check appear in the check box **Store Timestamps (This time takes effect immediately)**. Removing the check will disable timestamping.

7.1.4.3 Changing the Timestamp Resolution

This option affects the resolution of the timestamp stored in the capture file. The default timestamp is 10 milliseconds. This value is determined by the operating system and is the smallest "normal" resolutions possible.

Note: The raw timestamp value is the number of 100-nanosecond intervals since the beginning of January 1, 1601. This is standard Windows time.

It is also possible to use "high resolution" timestamping. High resolution timestamp values are marked by an asterisk as high resolution in the drop down list. To change timestamping resolutions:


Store Timestamps (This item takes effect immediately)
Capture Options
Storage Resolution: 0.50 Microseconds (high resolution)
Note 1: To apply resolution changes, you must restart the program.
Note 2: Finer resolutions increase the capture file size.

1. Go to the **Capture Options** section of the window.
2. Change the resolution listed in the **Storage Resolution** box.

Note: If you change the resolution, you need to exit the analyzer and restart in order for the change to take effect.

7.1.4.3.1 Performance Issues with High Resolution Timestamp

There are two things to be aware of when using high resolution timestamps. The first is that high resolution timestamps take up more space in the capture file because more bits are required to store the timestamp. Also, more timestamps need to be stored than at normal resolutions. The second issue is that using high resolution timestamping may affect performance on slower machines

For example, if 10 bytes of data are captured in 10 milliseconds at a rate of 1 byte per millisecond, and the timestamp resolution is 10 milliseconds, then only one timestamp needs to be stored for the 10 bytes of data. If the resolution is 1 millisecond, then 10 timestamps need to be stored, one for each byte of data. If you have two capture files, both of the same size, but one was captured using normal resolution timestamping and the other using high resolution, the normal resolution file has more data events in it, because less room is used to store timestamps.

You can increase the size of your capture file in the System Settings.

7.1.4.4 Switching Between Relative and Absolute Time

With Timestamping you can choose to employ Relative Time or Absolute time.

1. Choose **System Settings** from the **Options** menu on the **Control** window, and click the **Timestamping Options** button, or click the click the **Timestamping Options** icon from the **Event Display** window.
2. Go to the **Display Options** section at the bottom of the window and find the **Display Relative Timestamps** checkbox.
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

Note: The options in this section affect only how the timestamps are displayed on the screen, not how the timestamps are recorded in the capture file.

- **Display Raw Timestamp Value** shows the timestamp as the total time in hundred nanoseconds from a specific point in time.
- **Display Relative Timestamps** shows the timestamp as the amount of time that has passed since the first byte was captured. It works just like a stop watch in that the timestamp for the first byte is 0:00:00.0000 and all subsequent timestamps increment from there. The timestamp is recorded as the actual time, so you can flip back and forth between relative and actual time as needed.
- Selecting both values displays the total time in nanoseconds from the start of the capture as opposed to a specific point in time.
- Selecting neither value displays the actual chronological time.

When you select **Display Relative Timestamp** you can set the number of digits to display using the up or down arrows on the numeric list.

7.1.4.5 Displaying Fractions of a Second

1. Choose **System Settings** from the **Options** menu on the **Control** window, and click the **Timestamping Options** button, or click the click the **Timestamping Options** icon from the **Event Display** window.
2. Go to the **Display Options** section at the bottom of the window, and find the **Number of Digits to Display** box.
3. Click on the arrows to change the number. You can display between 0 and 6 digits to the right of the decimal point.

7.2 Technical Information

7.2.1 Performance Notes

As a software-based product, the speed of your computer's processor affects the analyzer's performance. Buffer overflow errors are an indicator that the analyzer is unable to keep up with the data. The information below describes what happens to the data as it arrives, what the error means, and how various aspects of the analyzer affect performance. Also included are suggestions on how to improve performance.

The analyzer's driver takes data from the driver and counts each byte as they are put into the driver's buffer. The analyzer's driver tells the user interface that data is ready to be processed. The analyzer takes the data from the driver's buffer and puts the data into the capture buffer.

Driver Buffer Overflows occur when the user interface does not retrieve frames from the driver quickly enough. Buffer overflows are indicated in the **Event Display** window by a plus sign within a circle. Clicking on the buffer overflow symbol displays how many frames have been lost.

There are several things that you can do to try and solve this problem.

- Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by the analyzer. (Ethernet Only)
- Close all other programs that are doing work while the analyzer is running. Refrain from doing searches in the **Event Display** window or other processor intensive activities while the analyzer is capturing data.
- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the file. Try turning off timestamping from the Timestamping Options window.
- For **Driver Buffer Overflows**, change the size of the driver buffer. This value is changed from the **Advanced System Settings**. Go to the **Control** window and choose **System Settings** from the **Options** menu. Click on the **Advanced** button. Find the value D**river Receive Buffer Size in Operating System Pages**. Take the number listed there and double it.
- The analyzer's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause the analyzer to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the **Event Display** and **Frame Display** windows. The analyzer can capture data with no windows other than the **Control** window open.

- If you are still experiencing buffer overflows after trying all of the above options, then you need to use a faster PC.

7.2.2 Ring Indicator

The following information applies when operating the analyzer in **Spy** mode or **Source DTE, No FTS Cables** mode. When using the cables supplied with the analyzer to capture or source data, Ring Indicator (RI) is routed to a different pin which generates interrupts normally.

There is a special case involving Ring Indicator and computers with 8250 UARTs or UARTs from that family where the state of RI may not be captured accurately. Normally when a control signal changes state from high to low or low to high, an interrupt is generated by the UART, and the analyzer goes to see what has changed and record it. Ring Indicator works a little differently. An interrupt is generated when RI changes from high to low, but not when RI changes from low to high. If Ring Indicator changes from low to high, the analyzer does not know that RI has changed state until another event occurs that generates an interrupt. This is simply the way the UART works, and is not a deficiency in the analyzer software.

To minimize the chance of missing a Ring Indicator change, the analyzer polls the UART every millisecond to see if RI has changed. It is still possible for the analyzer to miss a Ring Indicator change if RI and only RI changes state more than once per millisecond.

UARTs in the 8250 family include 8250s, 16450s, 16550s and 16550 variants. If you have any questions about the behavior of your UART and Ring Indicator, please contact technical support.

7.2.3 Progress Bars

The analyzer uses progress bars to indicate the progress of a number of different processes. Some progress bars (such as the filtering progress bar) remain visible, while others are hidden.

The title on the progress bar indicates the process underway.

7.2.4 Event Numbering

This section provides information about how events are numbered when they are first captured and how this affects the display windows in the analyzer. The information in this section applies to frame numbering as well.

When the analyzer captures an event, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8 of 11 when viewing only the data bytes.

The numbers assigned to events that are wrapped out of the buffer are not reassigned. In other words, when event number 1 is wrapped out of the buffer, event number 2 is not renumbered to event 1. This means that the first event in the buffer may be listed as event 11520 of 16334, because events 1-11519 have been wrapped out of the buffer. Since row numbers refer to the event numbers, they work the same way. In the above example, the first row would be listed as 2d00 (which is hex for 11520.)

The advantage of not renumbering events is that you can save a portion of a capture file, send it to a colleague, and tell your colleague to look at a particular event. Since the events are not renumbered, your colleague's file use the same event numbers that your file does.

7.2.5 Useful Character Tables

7.2.5.1 ASCII Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

7.2.5.2 Baudot Codes

DEC	HEX	LETTERS	FIGURES
0	00	BLANK (NUL)	BLANK (NUL)
1	01	E	3
2	02	LF	LF
3	03	A	-
4	04	SP	SP
5	05	S	BEL
6	06	I	8
7	07	U	7
8	08	CR	CR
9	09	D	$
10	0A	R	4
11	0B	J	'
12	0C	N	,
13	0D	F	!
14	0E	C	:
15	0F	K	(
16	10	T	5
17	11	Z	"
18	12	L	)
19	13	W	2
20	14	H	#
21	15	Y	6
22	16	P	0
23	17	Q	1
24	18	O	9
25	19	B	?
26	1A	G	&
27	1B	FIGURES	FIGURES
28	1C	M	.
29	1D	X	/
30	1E	V	;
31	1F	LETTERS	LETTERS

7.2.5.3 EBCDIC Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	TM	RES	NL	BS	IL	CAN	EM	CC	CU1	IFS	IGS	IRS	IUS
2x	DS	SOS	FS		BYP	LF	ETB	ESC			SM	CU2		ENQ	ACK	BEL
3x			SYN		PN	RS	UC	EOT				CU3	DC4	NAK		SUB
4x	SP											.	<	(	+	
5x	&										!	$	*	)	;	^
6x	-	/									|	,	%	_	>	?
7x										`	:	#	@	'	=	"
8x		a	b	c	d	e	f	g	h	i						
9x		j	k	l	m	n	o	p	q	r						
Ax		~	s	t	u	v	w	x	y	z				[		
Bx														]		
Cx	{	A	B	C	D	E	F	G	H	I						
Dx	}	J	K	L	M	N	O	P	Q	R						
Ex	\		S	T	U	V	W	X	Y	Z						
Fx	0	1	2	3	4	5	6	7	8	9						

7.2.5.4 Communication Control Characters

Listed below in alphabetical order are the expanded text meanings for common ANSI communication control characters, and two-character system abbreviation for each one. Some abbreviations have forward slash characters between the two letters. This is to differentiate the abbreviations for a control character from a hex number. For example, the abbreviation for Form Feed is listed as F/F, to differentiate it from the hex number FF.

Table 7.2 - Communications Control Characters

Abbreviation	Control Character	Text
AK	ACK	Acknowledge
BL	BEL	Bell
BS	BS	Backspace
CN	CAN	Cancel
CR	CR	Carriage Return
D/1-4	DC1-4	Device Control 1-4
D/E	DEL	Delete
DL	DLE	Data Link Escape
EM	EM	End of Medium
EQ	ENQ	Enquiry
ET	EOT	End of Transmission
E/C	ESC	Escape
E/B	ETB	End of Transmission Block
EX	ETX	End of Text
F/F	FF	Form Feed

Table 7.2 - Communications Control Characters(continued)

Abbreviation	Control Character	Text
FS	FS	File Separator
GS	GS	Group Separator
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle
US	US	Unit Separator
VT	VT	Vertical Tabulation

7.2.6 The Frontline Serial Driver

ComProbe software uses custom versions of the standard Windows serial drivers in order to capture data. These drivers are usually installed during the routine product installation. However, if you need to install the serial driver after ComProbe software has already been installed, please refer to the instructions available in the Setup folder installed under Start | Programs | [Product Name and version #] | Setup | How to Install the FTS Serial Driver.

7.2.7 DecoderScript Overview

The DecoderScript™ Reference Manual and User Guide is delivered with each Frontline ComProbe® Protocol Analysis System installation package under Developer Tools. The manual is also available on-line at FTE.com.

The main purpose of this manual is to describe DecoderScript™, the language used in writing decoders. DecoderScript allows you to create new decoders or modify existing decoders to expand the functionality of your ComProbe protocol analyzer. DecoderScript displays protocol data, checks the values of fields, validates checksums, converts and combines field values for convenient presentation. Decoders can also be augmented with custom C++-coded functions, called "methods", to extend data formatting, validation, transformations, and so on.

A decoder defines field-by-field how a protocol message can be taken apart and displayed. The core of each "decoder" is a program that defines how the protocol data is broken up into fields and displayed in the Frame Display window of the analyzer software.

This manual provides instruction on how to create and use custom decoders. When reading the manual for the first time, we encourage you to read the chapters in sequence. The chapters are organized in such a way to introduce you to DecoderScript writing step- by- step.

Screenshots of the ComProbe protocol analyzer have been included in the manual to illustrate what you see on your own screen as you develop decoders. But you should be aware for various reasons, the examples may be slightly different from the ones that you create. The differences could be the result of configuration differences or because you are running a newer version of the program. Do not worry if an icon seems to be missing, a font is different, or even if the entire color scheme appears to have changed. The examples are still valid.

Examples of decoders, methods, and frame recognizers are included in this manual. You can cut and paste from these examples to create your own decoders.

A quick note here: Usually the pasted code appears the same as the original in your editor. Some editors, however, change the appearance of the text when it is pasted (something to do with whether it is ASCII or Unicode text). If you find that the pasted text does not appear the same as the original, you can transfer the code into a simple text editor like Notepad, save it as an ANSI (ASCII) file, then use it in your decoder.

These files are installed in the FTE directory of the system Common Files directory. The readme file in the root directory of the protocol analyzer installation contains a complete list of included files. Most files are located in My Decoders and My Methods.

We will be updating our web site with new and updated utilities, etc, on a regular basis and we urge decoder writers to check there occasionally.

7.2.8 *Bluetooth* low energy ATT Decoder Handle Mapping

Low energy device attributes contain a 16-bit address called the attribute handle. Each handle is associated with an attribute Universally Unique Identifier (UUID) that is 128-bits long. In the attribute database, the handle is unique while the UUID is not unique.

The ComProbe software detects and stores the relationships (mappings) between handle and UUID during the GATT discovery process. But sometimes, there is no GATT discovery process because

- The discovery has previously taken place and both devices stored the mappings and the discovery will not repeat at every subsequent connection.
- The developer owns both devices in the conversation and chose to ignore discovery because the mappings are known.
- The devices are in development and the code to perform the mappings has not been written yet.

The solution to this problem is to

1. define the mappings in a file and
2. then pre-loading the mapping using the ComProbe software.

Creating handle-UUID mapping file

Create a file named "ATT_Handle_UUID_Preload.ini' in the root directory of "C:\Users\Public\Public Documents\Frontline Test Equipment\My Decoders\", but the file can be located anywhere.

Assume that you want to create a GATT service starting at handle 1.

Create a section in the ini file called

[Service Base Handles]

```
A=1
```

"A" will be your first service. Make the base handle equal to the handle of your service. You can use all upper and lower case letters so you can have up to 52 service handles.

Next add the following section.

```
[Advertiser Handles]
; Generic Access Profile (GAP)
A0 = 1800
A1 = 2803
A2 = 2a00
A3 = 2803
A4 = 2a01
A5 = 2803
A6 = 2a04
```

A few tings of note:

- In the code above, lines begging with a semi-colon are comments.
- If you want to change the base handle of the GAP service, change the "1" to some other number.
- If you want to comment out the entire service, comment out the base handle. If no "A" is defined, the software will ignore "A1", "A2" and so on.

7.3 Contacting Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

On the Web: http://fte.com/support/supportrequest.aspx

Email: tech_support@fte.com

If you need to talk to a technical support representative about your ComProbe 802.11 product, support is available between 9 am and 5 pm, U.S. Eastern Time zone, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

Instructional Videos

Frontline provides a series of videos to assist the user and may answer your questions. These videos can be accessed at fte.com/support/videos.aspx. On this web page use the **Video Filters** sidebar to select instructional videos for your product.

Appendicies

Appendix A: Application Notes **191**

Appendix A: Application Notes

A.1 802.11 Conductive Testing-Isolating the Environment 193

A.2 ComProbe Automation Server: Why use it? 195

A.1 802.11 Conductive Testing-Isolating the Environment

Conductive testing could be used for many reasons, but the most common use is to isolate the 802.11 Wi-Fi test setup from the surrounding environment. Interference from radio frequency (RF) sources is the most common reason for isolating the test from the environment. This is especially important when the environment contains RF sources using the industrial, scientific, and medical (ISM) radio bands used for Wi-Fi.

"Conductive" in this context means that you are not "air sniffing", that is, capturing 802.11 transmissions on the ComProbe 802,11 analyzer antenna. The conductive test setup uses coaxial cable to directly connect the Device Under Test (DUT) to the analyzer antenna connectors. The coaxial cable provides the isolation from the environment through shielding.

A.1.1 Test Equipment

The following equipment is required for the test setup. All cables, connectors and adapters, and attenuators should be relatively flat from 2 GHz to 6 GHz.

1. Coaxial cable All cable must be 50Ω and should be double shielded.
2. Coaxial T-connectors, 50Ω.
3. RP.SMA adapters for connecting coaxial cable or attenuators to the antenna connectors, 50Ω.
4. AT1 - AT9: 20 dB attenuators, 50Ω.
5. Frontline ComProbe 802.11 analyzer.
6. Computer for running ComProbe software.

A.1.2 Test Setup - 802.11

The following figure show the conductive test setup. For information on setting up and operating the ComProbe 802.11, refer to the ComProbe User Manuals at fte.com.

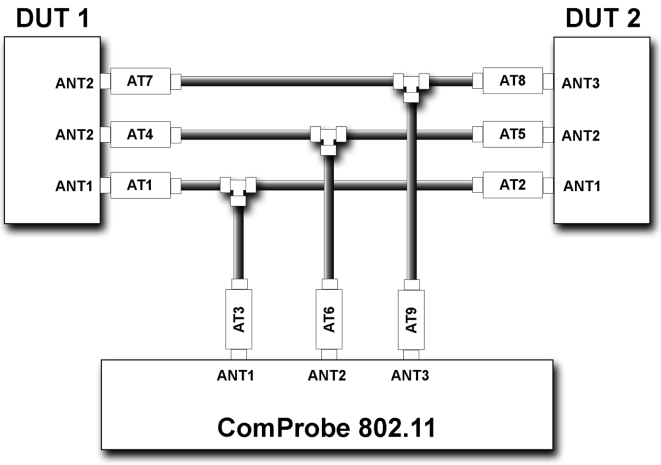


Figure A.1 - ComProbe 802.11 Conductive Test Setup for 3X3 MIMO

The above test setup if for 3X3 MIMO 802.11 devices. If not testing this configuration, the ANT3 connection to the DUTs and the ComProbe 802.11 is not used.

A.1.3 Test Process

After connecting DUT1, DUT2, and the ComProbe 802.11 , follow these steps to capture *Bluetooth* data.

1. Establish data transmission between DUT 1 and DUT 2.
2. Begin capture of the data with the ComProbe 802.11 . (Refer to the ComProbe 802.11 User Manual at fte.com.)
3. Conduct protocol analysis with the ComProbe software on the personal computer or save the capture file for future analysis.

For any questions concerning conductive testing, contact Frontline technical support at 434-984-4500 or email tech_support@fte.com.

Copyright 2015 Frontline Test Equipment, Inc.

Author: John Trinkle with Sean Clinchy

Publish Date: 19 October 2015

A.2 ComProbe Automation Server: Why use it?

Frontline provides a full line of wireless sniffing devices for developers that include ComProbe BPA 600 for Bluetooth® Classic, low energy, and coexistence; ComProbe 802.11 for Wi-Fi and *Bluetooth* coexistence. Normal ComProbe protocol analyzer use is through a GUI on a personal computer In this operation mode the user has direct control of the setup and data capture through the keyboard and mouse. User specific ComProbe analyzer configuration and capture decisions may come from user prescribed test documents or applied ad hoc or on-the-fly.

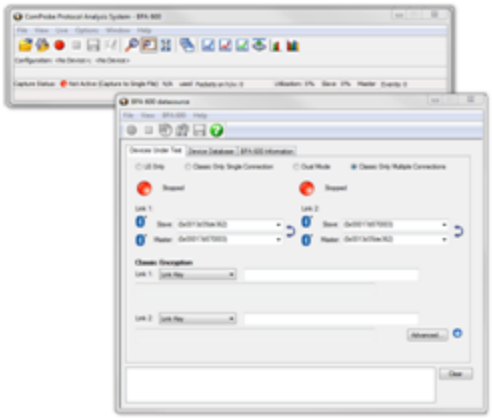


Figure 2 - ComProbe GUI

The ComProbe software GUI is sufficient for many development projects. But situations may arise where a more automated process is desirable. For example, if a company wants to ensure exact test processes, automating those processes is one answer. When testing multiple devices long test runs can occur, and automating can free up personnel to perform additional tasks. This is a list of possible situations when automation would improve testing and developments operations and save money.

- Automate long test runs – free up personnel for other tasking or run overnight.
- Automatic bookmarking capture data for specific events – helps developers focus on specific rest results.
- Automatic adherence to test procedures – ensures test repeatability and eliminates human error.
- Automatic exporting captured data – extracting specific data for post testing analysis outside of the ComProbe software, e.g. export to CSV.
- Automate other Windows – based applications while capturing data – for example, controlling other testing equipment related to the test.
- Automate regression testing.

The larger your task size the more benefit realized in cost avoidance and efficient resource usage through automation of the Frontline ComProbe protocol analyzers. The extra effort to program the test automation is minimal compared to the time saved to manually test.

Frontline's Automation Server provides the means to programmatically control ComProbe software and hardware in a client-server configuration. The Automation Server is provided when you purchase your ComProbe analyzer, and is stored in the Frontline ComProbe Protocol Analysis System directory. The ComProbe Automation Server Protocol Programmers Guide is located in this same directory. The process for automating your data capture is accomplished in three steps.

1. Connect the ComProbe hardware to a computer running ComProbe software and the Automation Server.
2. Launch the Automation Server program. The program will listen to the commands from the Automation Client program and according control the ComProbe software.
3. Write your Automation Client program (use the template provided with the installation package) and run it.

As long as there is no change in the programmed capture process, step 3 can be repeated reliably and without deviation. Should the test plan change, the program written in step 1 can serve as a template to minimze development timeand to provide quality control tracability.

A.2.1 Automation Server Topology

The Automation Server executes the commands issued by a user-created Automation client script. The client script can run either on the local PC or on a remote over a TCP/IP connection. The Automation Client program can be written in any language and uses the syntax defined in the ComProbe Automation Server Protocol Programmers Guide. The client will bypass the local Microsoft Windows interface and interacts directly with ComProbe software. One or more instances of the ComProbe software must be running along with one instance of the Automation Server.

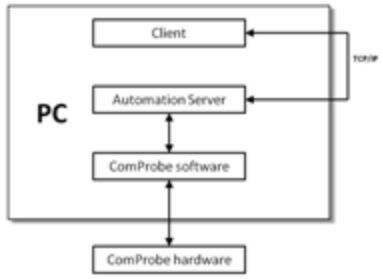


Figure 3 - Automation Server on a Single PC

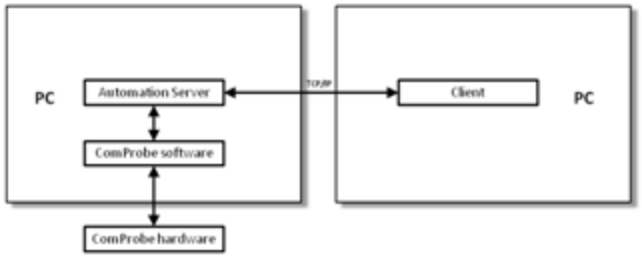


Figure 4 - Automation Server Using Two PCs

A.2.2 Writing Automation Script

Automation scripting is done by persons with knowledge of TCP socket communications. The process automation is achieved by writing a client application which talks over a TCP network socket connection with the ComProbe Automation Server.

Delivered in your ComProbe installation package is a sample script SampleClient.tcl. This script is located in your installation directory. This is typically located at C:\Program Files (x86)\Frontline Test System II\Frontline ComProbe Protocol Analysis System *[your version]*\Development Tools\. On 32-bit Windows or Windows XP the root installation folder is "C:\Program Files\".

The sample script is written in TCL (Tool Command Language). TCL is an open-source, cross-platform programming language. More information is available at www.tcl.tk. The script can be translated to any general purpose programming language such as C# as long as you retain the program structure.

The sample script is divided into the following sections identified by comments "#".

```
##########################################################
# Procedures
##########################################################
```

1. Procedures
2. Command Wrappers
3. FTE_Base namespace vars
4. Start of Sample Script

Do not change any script in Procedures and Command Wrappers.

FTE_Base namespace vars Modifications

In the "FTE_Base namespace vars" section you will need to identify the connections for the host and the port. Near the top of this section locate the following code at or near line number 747 - 748.

```
set Connections(Host) 0.0.0.0;
set Connections(Port) 22901;
```

For the Host, change 0.0.0.0 to the IP address of the computer running Automation Server. For example 192.168.10.94.

For the Port number, the default is set to 22901, which is not a common TCP port. It is unlikely that another application is using this port, so you can leave the Port set to default 22901.

Note: Before launching the Automation Server, the IP address and IP port—the same as the script Host and Port values—must be modified in the XML configuration file *FTSAutoServer.exe.config*. This file is located in C:\Program Files\Frontline Test System II\Frontline ComProbe Protocol Analysis System *[your version]*\Executable\Core\ directory. The code to modify is <add key="IPAddr" value="0.0.0.0"/> and <add key="Port" value="22901"/>

Start of Sample Script Modifications

This section is the main part of the program and several lines in the template need to be changed to support your unique data capture environment. First at or around line 792 we need to input the Host IP address again. Locate the following code and enter your Host IP address. FTEBaseInit is a procedure that sets up the TCP connection.

```
FTEBaseInit 192.168.0.90
```

At or around line 803 change "13.1.830.1052" in the following code to the version of your ComProbe software. The version number can be found listed with your Frontline installation directory at C:\Program Files (x86) \Frontline Test System II\. CPASVersion is a varible used in the program to locate your installed version of the ComProbe software.

```
set CPASVersion "C:\\Program Files\\Frontline Test System II\\Frontline ComProbe Protocol Analysis
    System 13.1.830.1052\\Executables\\Core"
```

Lastly, you need to identify the "personality" of the ComProbe hardware. On or about line 823 you will change the following code to replace the text within the quotes with the personality key that matches your sniffing hardware configuration. Within the sample script are a few examples of commonly used personalities or "profiles". The Programmers Guide provides a complete list of personalities.

```
set Profile "BPA600_Coex"
```

This code is the personality for using a ComProbe BPA 600 for Classic Bluetooth and a ComProbe 802.11 for Wi-Fi with the software operating in Coexistence View. If you wanted to use just the ComProbe BPA 600 for captureing Classic Bluetooth and Bluetooth low energy then you would change the value in quotes to "BPA600".

Having made these changes to the sample script template you are ready to capture data using your client-server configuration, TCP connection, and capture hardware. At this point you shouild save the sample script as your own template. As long as you maintain this test setup you will not need to change these settings making your unique template reusable. However you may want to build a library of templates to cover a variety of automation configurations. Once your unique template is coded you will find that development time for variations to the template is insignificant.

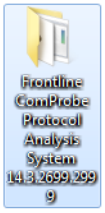
In the next section we will step through the remainder of the sample script program to show how the Automation Server converts the sniffing process to a largely self -acting process.

A.2.3 Running Automation Server Script

In this section we will make a comparison between the main program code and the manual operation at the GUI in a sniffing and capture session. This approach will show that the Automation Server will duplicate the manual processes but automation offers reliable repetition of those manual process and will save time in development and regression testing.

Note: Note that this is sample script and that you will have to change the code in the main program to suit your specific sniffing and capture needs. The command set is outlined in the Programmers Guide in Chapter 3.

On or about line 824 of the sample script you will see the following code. StaertFTS tells the Automation Server to launch the ComProbe software by opening your version of Frontline ComProbe Protocol Analysis System and to use a specific personality.




```
StartFTS [format "%s;%s" $CPASVersion $Profile]
```

In the code above from the sample script $CPASVersion was defined at line 803, and the $Profile was set at line 823 to use ComProbe BPA 600 and ComProbe 802.11 in coexistence. This is equivalent to 1) double clicking on the Frontline desktop folder and starting the software and 2) selecting a capture method.

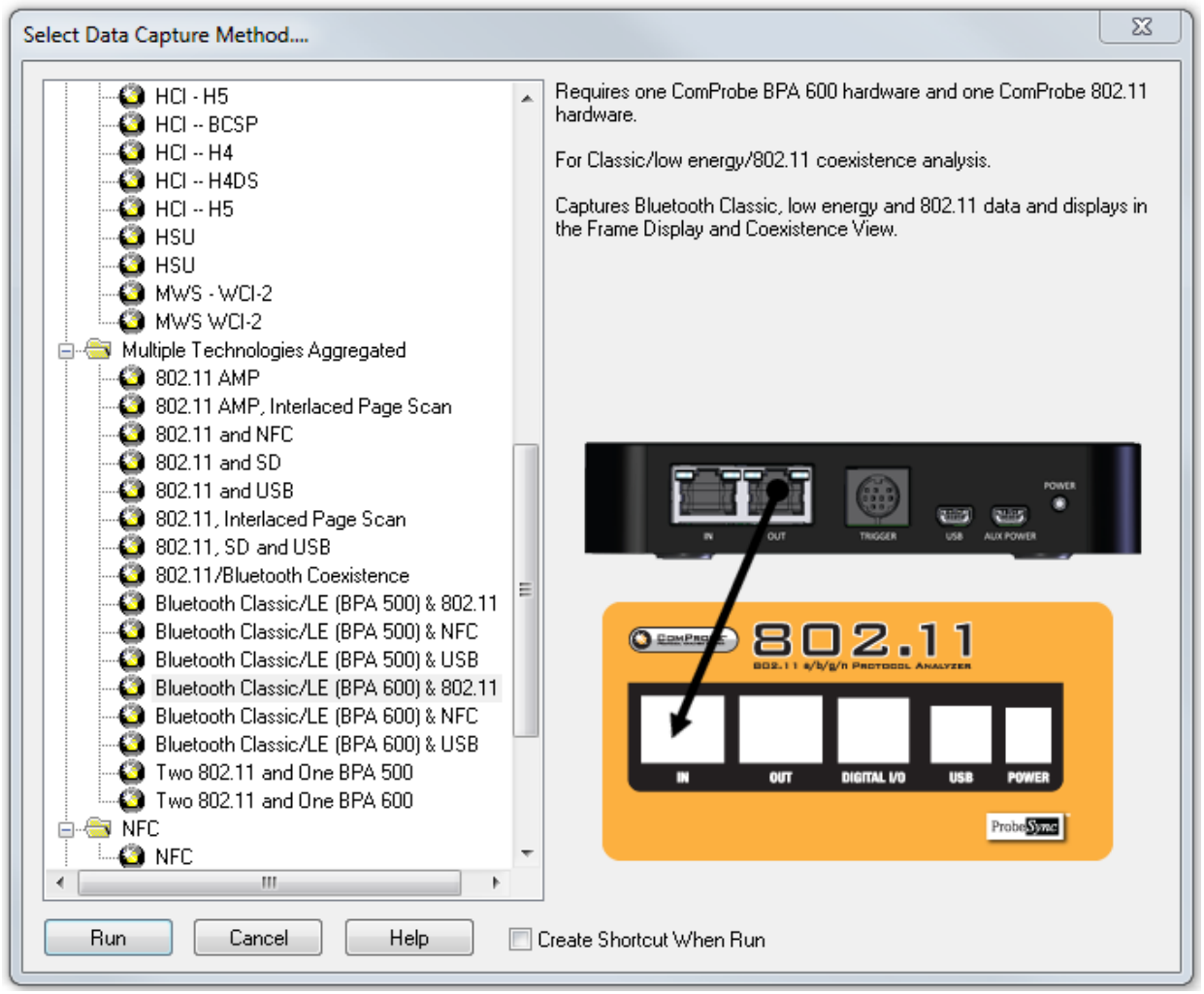


Figure 5 - $Profile = BPA600_Coex", BPA600 and 802.11 in Coexistence

Moving to line 831 in the sample script we see a configuration setting command for the ComProbe BPA 600. The only parameters shown in this code are the address of the Master and Slave devices. If other parameters are omitted from the code the default values are selected. This line of code is equivalent to setting the BPA 600 datasource for Classic Bluetooth.

```
ConfigSettings [format "IOParameters;BPA600;Master=0x00025b01cb8b;Slave=0x00025b01cbe1"]
```

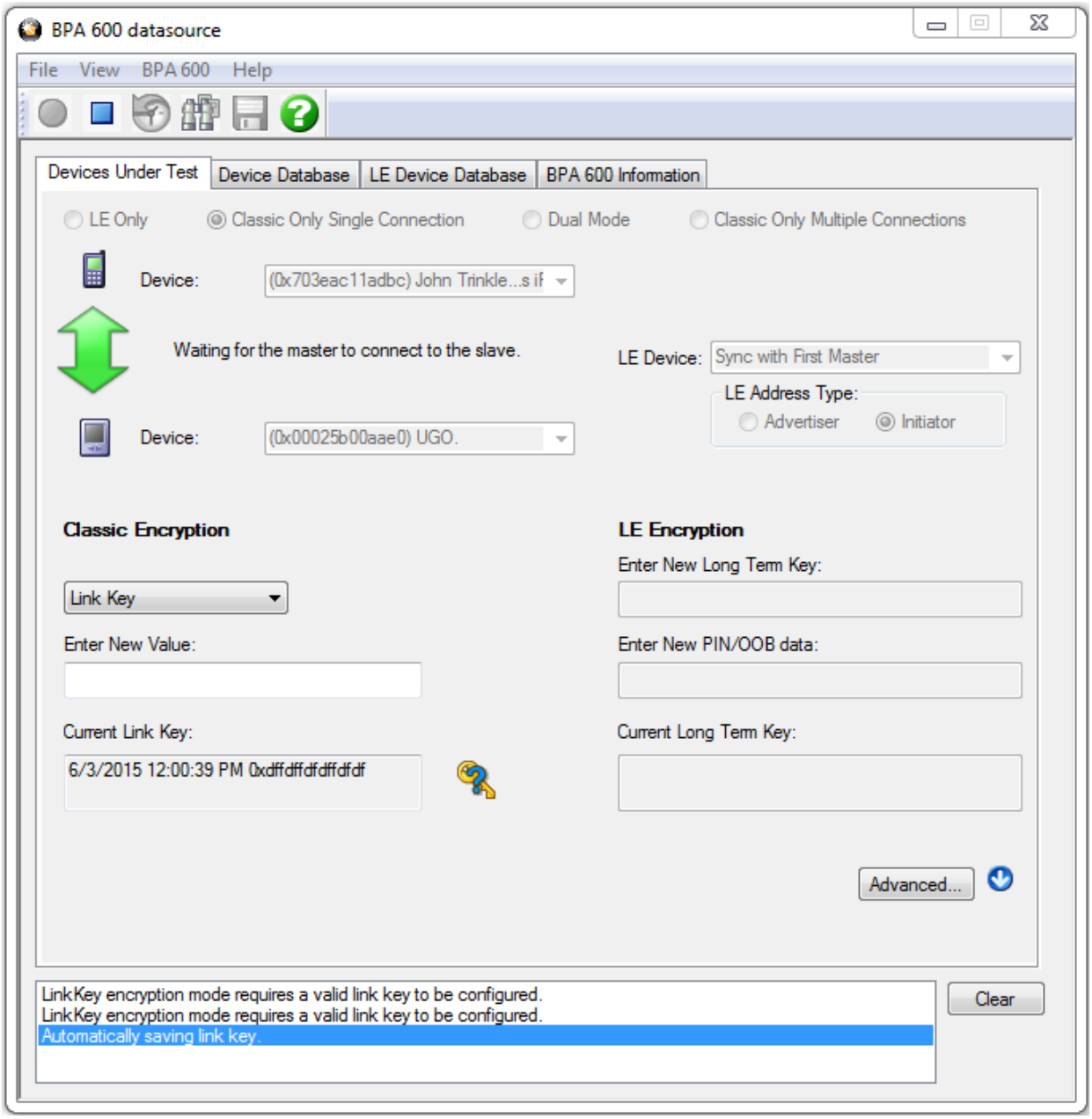


Figure 6 - ConfigSettings equivalent: ComProbe BPA 600 Configuration Settings Dialog

Similar ConfigSettings code will appear in the sample script for the ComProbe 802.11.

At line 853 the StartSniffing command appears. This is equivalent to clicking the **Start Sniffing** button on the **BPA 600 datasource** toolbar. Start Sniffing will start synchronization of the BPA 600 with the *Bluetooth* Devices. Once synchronization is acheived the arrow between the Classic devices will turn green with the arrow head point to the master device.

```
StartSniffing
```

Note: StartSniffing is unique to *Bluetooth* ComProbe devices, and it will automatically execute the Automation Server StartCapture command once synchronized. For non-*Bluetooth* devices use the StartCapture command that is equivalent to the Start Capture button in the Control window.

At line 874 the following code will halt the capture after 10 seconds. This bit of code illustrates the control that you can have over the capture process.

```
after 10000
```

At line 879 we have another *Bluetooth*-unique command that stops the sniffing and is equivalent to clicking the Stop Sniffing button on the BPA 600 datasource.

```
StopSniffing
```

Here is one of those *Bluetooth*-unique situations. At line 889 the Stop Capture command is issued. Unlike the Start Sniffing command , the Stop Sniffing command does not automatically execute the Stop Capture command so it must be in the program if using ComProbe *Bluetooth* hardware. Stop Capture will stop the capture of data. This command is equivalent to clicking on the **Stop Capture** button on the **Contrtol** window.

```
StopCapture
```

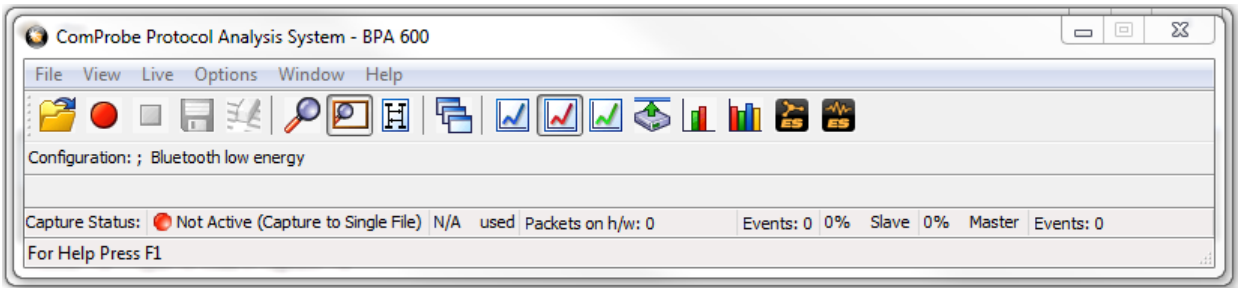

ComProbe Protocol Analysis System - BPA 600
File View Live Options Window Help
Configuration: ; Bluetooth low energy
Capture Status: Not Active (Capture to Single File) N/A used Packets on h/w: 0 Events: 0 0% Slave 0% Master Events: 0
For Help Press F1

Figure 7 - BPA 600 **Control** window; **Stop Capture** is to the right of the red button.

At the end of the program you will want to stop the ComProbe software, so at line 900 we have the following code.

```
StopFTS
```

Finally good programming housekeeping dictates that you should clear all connections. The following procedure will disconnect the client-server and breakdown the TCP connection.

```
FTEBaseCleanup
```

This section has hit only the highlights of the sample script, but it has illustrated the connection between Automation and the manual sniffing and capture of data. Your programs may be more detailed and will certainly use many more commands. Refer to the ComProbe Automation Server Protocol Programmers Guide for more information on the command set.

A.2.4 Saving Automation Captured Data

The Automation Server sample script gives you a building block for building your ComProbe hardware and software sniffing and data capture process. Of course the primary purpose for using ComProbe products may be to analyze the captured data to solve design and development issues, and to test your products. The sample script does not provide sample code for the saving and exporting of the captured data.

The Save Capture command is equivalent to clicking on the ComProbe software **Control** window **File** menu **Save** selection. The **Save** selection opens a Save as dialog where you would enter the location and file name for your capture data—a .cfa file. The Save Capture command contains parameters that perform the same operation only automatically.

Save Capture;c:Users\Public\Public documents\Frontline Test Equipment\My Capture Files\mycap.cfa

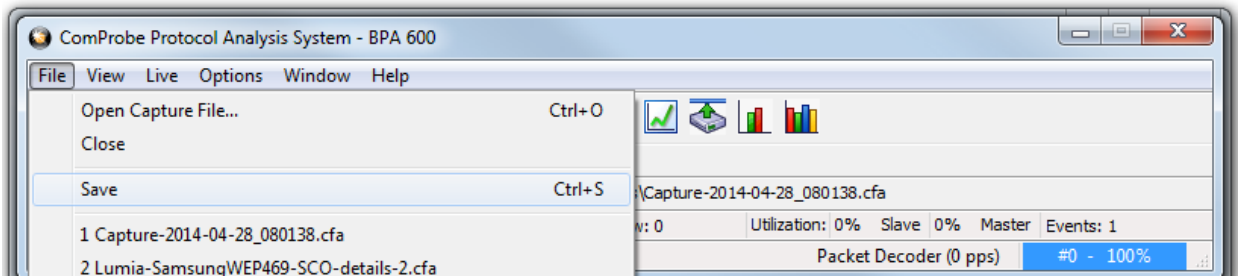


Figure 8 - ComProbe Software **File Save**

Save Capture command will save the entire capture file, which can be reloaded into the ComProbe software for later analysis. To reload the capture file you use the Automation Server Open Capture File command that has similar parameters to the Save Capture command.

Open Capture File;c:\Users\Public\Public documents\Frontline Test Equipment\My Capture Files\mycap.cfa

While the Save Capture automatically archives everything that happened during the capture session your may want to write a script that focuses on specific protocols. To do that you use the Automation Server Export command that tells ComProbe software to invoke the **Frame Display** and then automatically selects the **File Export** menu option. In the example code below the data is exported to the identified path/file, is waiting for the frame to complete, and is selecting the 802.11 MAC protocol tab..

Export;c:\Users\Public\Public documents\Frontline Test Equipment\My Capture Files\mycap.csv;Mode=0;Tab=802.11:802.11 MAC

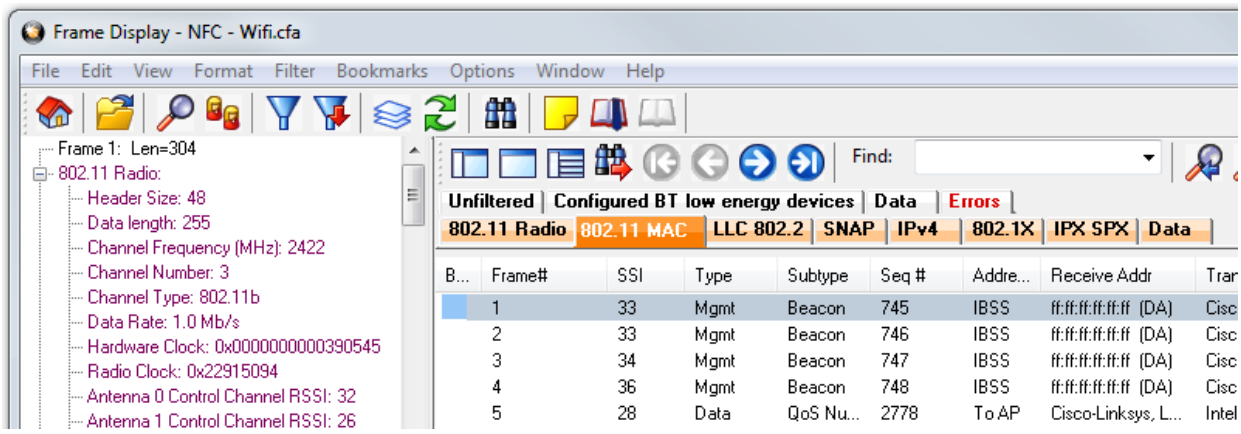

Frame Display - NFC - Wifi.cfa
File Edit View Format Filter Bookmarks Options Window Help
Frame 1: Len=304
802.11 Radio:
Header Size: 48
Data length: 255
Channel Frequency (MHz): 2422
Channel Number: 3
Channel Type: 802.11b
Data Rate: 1.0 Mb/s
Hardware Clock: 0x0000000000390545
Radio Clock: 0x22915094
Antenna 0 Control Channel RSSI: 32
Antenna 1 Control Channel RSSI: 26
Find:
Unfiltered Configured BT low energy devices Data Errors
802.11 Radio 802.11 MAC LLC 802.2 SNAP IPv4 802.1X IPX SPX Data
B... Frame# SSI Type Subtype Seq # Addre... Receive Addr Trar
1 33 Mgmt Beacon 745 IBSS ff:ff:ff:ff:ff:ff (DA) Cisc
2 33 Mgmt Beacon 746 IBSS ff:ff:ff:ff:ff:ff (DA) Cisc
3 34 Mgmt Beacon 747 IBSS ff:ff:ff:ff:ff:ff (DA) Cisc
4 36 Mgmt Beacon 748 IBSS ff:ff:ff:ff:ff:ff (DA) Cisc
5 28 Data QoS Nu... 2778 To AP Cisco-Linksys, L... Intel

Figure 9 - Export Command equivalent: Frame Display 802.11 MAC tab selected

Refer to the ComProbe Automation Server Protocol Programmers Guide for detail of the Export command Mode and Tab parameters.

Export provides you with the ability to automatically save specific protocol data that may be the focus of your analysis. The exported file is saved as a comma separate value (.csv) file type. This file may be opened for later analysis in any application that supports .csv format such as Micosoft Excel or Access.

A.2.5 Keeping Track of Events

Automation Server Add Bookmark command will automatically add a book mark to the last frame currently in the capture buffer.

Consider this scenario. You have set up your automation script but you want to keep track of the specific events, for example when you start streaming music from your smart phone to a *Bluetooth* speaker. The

```
Add Bookmark;String=StartMusicStream
```

In this scenario the Add Bookmark command may be used with TCL conditional statements to detect and guide the event actions. The string parameter will be the name on the bookmark for your saved or exported data capture. When analyzing the automated capture session at a later date you can use the bookmark to localize your analysis to the event.

A.2.6 Automation Can Save Time and Money

In a carefully considered design, development, or testing environment automation of wireless sniffing and data capture can save time and money. The Frontline Automation Server gives you the means to save time by ensuring process are reliably reproduced. This is especially true for situations when you want to run the identical tests on several products or versions of a product. Being able to compare captured data across design versions is enhanced when you can run exactly the same process.

Up-front automation script development time is a consideration when setting up an automated sniffing process. The ComProbe Automation Server Protocol Programmers Guide is delivered with your installation package, and the latest version is always available for download on FTE.com/support/documents in ComProbe Automation. Should you need additional assistance with the Automation Server, contact Frontline's technical support team.

Copyright 2015 Frontline Test Equipment, Inc.

Author: John Trinkle

Publish Date: 8 May 2014

The Bluetooth SIG, Inc owns the *Bluetooth* word mark and logos, and use of such marks is under license.

Index

8

802.11 I/O Settings 18

A

Aborted Frame 174

About Display Filters 80

Absolute Time 180

Add a New or Save an Existing Template 32

Adding a New Predefined Stack 48

Adding Comments To A Capture File 161

Advanced System Options 173

Apply Capture Filters 82

Apply Display Filters 80-83, 85

ASCII 57

- character set 182
- viewing data in 57

ASCII Codes 182

ASCII Pane 77

Auto-Sizing Column Widths 75

Automatically Request Missing Decoding Information 50

Automatically Restart 171

Automatically Restart Capturing After 'Clear Capture Buffer' 171

Automatically Save Imported Capture Files 171

Autotraversal 48, 50

B

Bar Charts 137

Baudot 57, 170

Baudot Codes 183

Begin Sync Character Strip 59

Binary 56, 143

Binary Pane 78

BL 184

Bookmarks 156-157

Boolean 83, 88

Broken Frame 58

BS 184

Buffer 160, 171

- Buffer Overflow 171
- Buffer Tabs 136
- Buffer/File Options 171

Byte 54, 56, 78, 182

- Searching 146

byte export 70

C

Calculating Data Rates and Delta Times 55

Capture Buffer 160, 171, 173

- Capture Buffer Size 171

Capture File 39, 160-163, 171, 173

- auto-save imported files 171
- capture to a series of files 171
- capture to one file 171
- changing default location of 175
- changing max size of 171, 173
- framing captured data 49
- importing 163
- loading 162
- reframing 49
- removing framing markers 49
- saving 160-161
- starting capture to file 39

Capturing 39
Data to Disk 39
CFA file 161-162
Changing Default File Locations 175
Character 143, 184
Character Pane 77
Character Set 57, 182-183
Characters Per Second Table 137
Choosing a Data Capture Method 7
Clear Capture Buffer 171
CN 184
Coexistence View 95
le Devices Radio Buttons 117
Legend 118
Set Button 116
Throughput Graph 108
Discontinuities 109
Dots 112
Swap Button 111
Viewport 110
Zoom Cursor 115
Zoomed 113
Freeze Y 114
Unfreeze Y 114
Y Scales Frozen 114
Throughput Indicators 105
Throughput Radio Buttons 117
Timeline Radio Buttons 117
Timelines 118
discontinuities 126
high-speed 127
packet 118
two timelines 123
Toolbar 103
Tooltip 109
relocate 109, 121
Color of Data Bytes 79
Colors 79
Comma Separated File 167
Compound Display Filters 83
Confirm CFA Changes 162
Context For Decoding 50
Control Characters 184
Control Signals 58, 177
Control Window 17, 171
Configuration Information 13
Conversation Filters 85
Copying Statistics 137
CPAS Control Window Toolbar 12
CR 184
CRC 54
CSV Files 167
Custom Protocol Stack 46, 48
Custom Stack 47-48
Customizing Fields in the Summary Pane 75

D

D/1 184
D/2 184
D/3 184
D/4 184
D/E 184

Data 55, 159-160
Capturing 39
Data Byte Color Denotation 79
Data Errors 152
Data Extraction 130
Data Rates 55
Decimal 56
Decode Pane 76
decoder 185
Decoder Parameters 30
DecoderScript 185
Decodes 29, 46, 51, 60, 66, 76, 140
Default File Locations 175
Delete a Template 32
Deleting Display Filters 85
Delta Times 55
Direction 85
Directories 175
Disabling 171
Display Filters 80, 86-88
Display Options 181
DL 184
Dots 76
Driver 185
Duplicate View 52, 54, 69-70

E

E/B 184
E/C 184
Easy Protocol Filtering 95
EBCDIC 57
EBCDIC Codes 183
EIR 46
EM 184
EQ 184
Errors 152, 177
ET 184
Event Display 51, 69, 167
Event Display Export 167
Event Display Toolbar 52
Event Numbering 182
Event Pane 78
Event Symbols 58
EX 184
Exclude 82
Exclude Radio Buttons 82
Expand All/Collapse All 76
Expand Decode Pane 70
Export
Export Baudot 170
Export Events 168
Export Filter Out 170
Extended Inquiry Response 46

F

F/F 184
FCSs 54
Field Width 75
File 159-162, 171
File Locations 175
File Series 171
File Types Supported 162
Filtering 94
Filters 80-83, 85-88, 95

Find 140, 143-144, 146-147, 152

Find - Bookmarks 154

Find Introduction 139

Font Size 60

Frame Display 60, 63, 66-67, 69-70, 75-79

Frame Display - Change Text Highlight Color 78

Frame Display - Find 67

Frame Display Status Bar 66

Frame Display Toolbar 63

Frame Display Window 61

Frame Recognizer Change 59

Frame Symbols 76

Frame Information on the Control Window 13

Freeze 55

FS 185

FTS Serial Driver 185

G

Go To 146

Graphs 138

Green Dots in Summary Pane 76

GS 184

H

Hardware Settings Overview 802.11 18, 27

Hex 56

Hexadecimal 77

Hiding Display Filters 85

Hiding Protocol Layers 66

High Resolution Timestamping 180

HT 185

I

I/O Settings 11

I/O Settings Change 59

Icons in Data on Event Display 58

Importable File Types 163

Importing Capture Files 162

INCLUDE 82

Include/Exclude 82

L

Layer Colors 79

LF 185

Live Update 55

Logical Byte Display 67

Logical Bytes 67

Long Break 59

Low Power 59

M

Main Window 11

Master 11

Minimizing 17

Mixed Channel/Sides 57

Mixed Sides Mode 57

Modem Lead Names 177

Modify Display Filters 87-88

Multiple Event Displays 54

Multiple Frame Displays 70

N

NK 184

Node Filters 85

Nonprintables 170

Notes 161

NU 184

Number Set 56

Numbers 182

O

Octal 56

Open 54

Open Capture File 162

Options 171, 173-174, 178

Other Term

Subterm 16

Overriding Frame Information 50

Overrun Errors 153

P

Panes 70

Pattern 142

Pause 39

Performance Notes 181

Pie Charts 137

Port Assignment 35

Printing 138, 166

Printing from the Frame Display 163

Progress Bars 182

Protocol

Protocol Layer Colors 79

Protocol Layer Filtering 94

Protocol Stack 47-48, 50

Q

Quick Filtering 94

R

Radix 56, 77

Reframe 49

Reframing 49

Relative Time 144, 180

Remove

Bookmarks 156-157

Columns 75

Custom Stack 47

Filters 85-86

Framing Markers 49

Reset Panes 70

Resetable Tab 136

Resolution 179

Resumed 58

Revealing Protocol Layers 66

RS 184

RSSI 28

S

Save 82, 159-161

Save As 159

Saving 160-161

Display Filter 81

Imported Capture Files 171

Saving the Capture File using File > Save or the Save icon 159

Search 140, 142, 144, 146-147, 152, 155-157

binary value 142

bookmarks 157

character string 142

errors 152

event number 147

frame number 146

hex pattern 142

pattern 142

special event 147

timestamp 144

wildcards 142
Security
802.11 I/O Settings 18
WPA Key 33
Seed Value 54
Serial Driver 185
Short Break 59
Side Names 177
Sides 177
Slave 11
Sorting Frames 67
Special Events 147
Start 58
Start Up Options 174
Statistics 133
Statistics Graphs 137
Summary 72
Summary Pane 72, 75-76
Sync Dropped 59
Sync Found 59
Sync Hunt Entered 59
Sync Lost 59
Synchronization 69
System Settings 171, 173

T

Technical Support 187
Test Device Began Responding 59
Test Device Stopped Responding 59
Timestamp 156, 179-180
Timestamping 156, 178, 180
Timestamping Disabled 59
Timestamping Enabled 59
Timestamping Options 171, 178
Timestamping Resolution 179
Timestamps 178, 180
Transferring Packets 39
Truncated Frame 59

U

Underrun Error 59
Unframe 49
Unframe Function 49
Unframing 49
Unknown Event 60

V

vendor specific decoder 185
Viewing Data Events 56

W

WEP
802.11 I/O Settings 18
Wi-Fi Timeline
Wi-Fi Error Statistics 137
WPA Key 33
802.11 I/O Settings 18
WPA Key 33
Wrap Buffer/File 171

Z

Zooming 125
zooming cursor 115